(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年4 月20 日 (20.04.2006)

PCT

(10) 国際公開番号
WO 2006/040910 A1

(51) 国際特許分類:
H04L 12/66 (2006.01)

(21) 国際出願番号: PCT/JP2005/017305

(22) 国際出願日: 2005 年9 月20 日 (20.09.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2004-298247
2004 年10 月12 日 (12.10.2004) JP
特願 2004-308554
2004 年10 月22 日 (22.10.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町二丁目３番１号 Tokyo (JP).

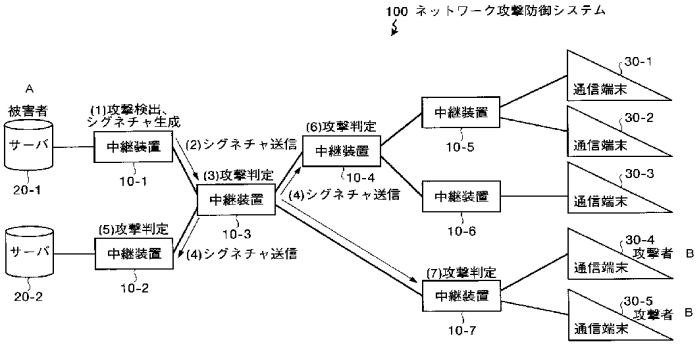
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 瀬林 克啓 (SEBAYASHI, Katsuhiro) [JP/JP]; 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 倉上 弘 (KURAKAMI, Hiroshi) [JP/JP]; 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 副島 裕司 (SOEJIMA, Yuji) [JP/JP]; 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). チェン エリック (CHEN, Eric) [CA/JP]; 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 冨士 仁 (FUJI, Hitoshi) [JP/JP]; 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

/続葉有/

(54) Title: REPEATER, REPEATING METHOD, REPEATING PROGRAM, AND NETWORK ATTACK DEFENDING SYSTEM

(54) 発明の名称: 中継装置、中継方法、中継プログラム並びにネットワーク攻撃防御システム



100... NETWORK ATTACK DEFENDING SYSTEM
A... VICTIM
20-1... SERVER
20-2... SERVER
(1)... ATTACK DETECTION AND SIGNATURE CREATION
10-1... REPEATER
(5)... ATTACK JUDGMENT
10-2... REPEATER
(2)... SIGNATURE SENDING
(3)... ATTACK JUDGMENT
10-3... REPEATER
(4)... SIGNATURE SENDING
(6)... ATTACK JUDGMENT
10-4... REPEATER
10-5... REPEATER
10-6... REPEATER
(7)... ATTACK JUDGMENT
10-7... REPEATER
30-1... COMMUNICATION TERMINAL
30-2... COMMUNICATION TERMINAL
30-3... COMMUNICATION TERMINAL
30-4... COMMUNICATION TERMINAL
B... ATTACKER
30-5... COMMUNICATION TERMINAL

(57) Abstract: On receiving a signature from an adjacent repeater, a repeater (10) judges whether or not the number of packets exceeds a predetermined threshold in a unit time satisfying the condition of the received signature. If the number is judged to exceed the threshold, the repeater (10) judges whether or not the number of consecutive excesses over the threshold exceeds a predetermined threshold. If the number of consecutive excesses exceeds the predetermined value, the repeater (10) sends the signature received from the adjacent repeater to the adjacent repeater other than the adjacent repeater which has sent the signature.

(57) 要約: 中継装置１０は、隣接中継装置からシグネチャを受信すると、受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定する。そして、中継装置１０は、単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する。このような判定の結果、所定の閾値を連続して超過した回数が所定値を超過したと判定された場

/続葉有/

WO 2006/040910 A1

(74) 代理人: 酒井 宏明, 外(SAKAI, Hiroaki et al.); 〒1006019 東京都千代田区霞が関三丁目２番５号 霞が関ビルディング 酒井国際特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

合に、中継装置１０は、隣接中継装置から受信したシグネチャを当該隣接中継装置を除く他の隣接中継装置に対して送信する。

明 細 書

中継装置、中継方法、中継プログラム並びにネットワーク攻撃防御システム

技術分野

[0001] この発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムに関する。

背景技術

[0002] 従来より、防御対象であるコンピュータが接続されたネットワーク上に複数の中継装置を有し、DoS(DenialofService)攻撃またはDDoS(DistributedDenialofService)攻撃を受けるコンピュータを防御するネットワーク攻撃防御システムが知られている。例えば、特許文献1(特開2003－283554号公報)や特許文献2(特開2003－283572号公報)に開示されたネットワーク攻撃防御システムでは、中継装置において、予め決められた攻撃容疑パケットの検出条件に通信トラヒックが合致するか否かをチェックする。そして、合致したトラヒックを検出した場合に、中継装置は、検出された攻撃容疑パケットの伝送帯域制限値を表すシグネチャを生成して隣接中継装置(隣接関係をもつ中継装置)へ送信するとともに、以後、シグネチャによって識別される攻撃容疑パケットの伝送帯域を制限する処理を行う。

[0003] 一方、シグネチャを受信した中継装置(隣接中継装置)では、通過するパケットの伝送帯域をシグネチャによって表される伝送帯域制限値に制限するとともに、さらに上流の隣接中継装置に対してシグネチャを送信する。つまり、シグネチャを受信した各中継装置がシグネチャの送信を繰り返すことで、ネットワーク上の全ての中継装置が同様のシグネチャに基づいてパケットを処理し、これによって、各中継装置を通過するパケットの伝送帯域をシグネチャが示す伝送帯域制限値に制限する。なお、上流または下流の中継装置とは、隣接中継装置であり、かつ攻撃容疑パケットが流入する方向に対する中継装置である。

[0004] さらに、一定時間経過後、攻撃を検出した中継装置は、各隣接中継装置から攻撃

容疑パケットの平均入力伝送帯域値を受信し、各隣接中継装置における平均入力伝送帯域の比率により伝送帯域制限調整値を算出し、算出した伝送帯域制限調整値を隣接中継装置に送信する。そして、かかる伝送帯域制限調整値を受信した中継装置は、受信した伝送帯域制限調整値に基づいて伝送帯域制限を調整しながら、さらに上流の隣接中継装置に伝送帯域制限調整値を送信する。つまり、伝送帯域制限調整値を受信した各中継装置が伝送帯域制限調整値の送信を繰り返すことで、ネットワーク上の全ての中継装置が同様の伝送帯域制限調整値を受信し、受信した伝送帯域制限調整値に基づいて伝送帯域制限を調整する。

[0005] 特許文献1:特開2003－283554号公報

特許文献2:特開2003－283572号公報

発明の開示

発明が解決しようとする課題

[0006] しかしながら、上記した従来の技術は、ネットワーク上の特定の中継装置が容疑のかかる攻撃を検出した場合でも、ネットワーク攻撃防御システムを構成する全ての中継装置に対してシグネチャを送信するので、攻撃容疑パケットの通信経路上にない中継装置にまでもシグネチャを送信してしまう結果、容疑のかかる攻撃を検出したとき等の各中継装置にかかる処理負荷が高くなってしまうという問題があった。

[0007] そこで、この発明は、上述した従来技術の課題を解決するためになされたものであり、ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能な中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムを提供することを目的とする。

課題を解決するための手段

[0008] 上述した課題を解決し、目的を達成するため、請求項1に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置であって、前記隣接中継装置から受信したシグネチャに基づいて当該シグネチャを他の隣接中継装置に送信すべきか否かを判定し、前記他の隣接中継装置に送信すべきと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

[0009] また、請求項2に係る発明は、前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手段と、前記攻撃有無判定手段によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手段と、を備えたことを特徴とする。

[0010] また、請求項3に係る発明は、上記の発明において、前記攻撃有無判定手段は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定手段を備え、前記シグネチャ送信手段は、前記パケット数判定手段によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

[0011] また、請求項4に係る発明は、上記の発明において、前記攻撃有無判定手段は、前記パケット数判定手段によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定手段をさらに備え、前記シグネチャ送信手段は、前記連続超過回数判定手段によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

[0012] また、請求項5に係る発明は、上記の発明において、前記シグネチャ送信手段は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする。

[0013] また、請求項6に係る発明は、上記の発明において、受信した前記シグネチャを記憶する記憶手段と、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、を備えたことを特徴とする。

[0014] また、請求項7に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする。

[0015] また、請求項8に係る発明は、上記の発明において、攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手段を備え、当該シグネチャ生成手段は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする。

[0016] また、請求項9に係る発明は、上記の発明において、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を他の隣接中継装置に送信するとともに、当該シグネチャの直前の中継元である隣接中継装置を特定するための中継元情報、当該シグネチャの直後の中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報および容疑シグネチャを前記シグネチャ記憶手段に対応付けて登録し、前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されている場合には、当該生成識別情報に対応付けて登録されている中継元情報が前記受信したシグネチャの中継元情報と同一であるか否かをさらに判定し、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に既に登録されているが、前記中継元情報が同一であると判定された場合には、前記隣接中

継装置から受信したシグネチャを前記シグネチャ記憶手段に上書き登録するとともに、当該シグネチャを前記シグネチャ記憶手段に登録されている中継先情報が示す他の隣接中継装置に送信することを特徴とする。

[0017] また、請求項10に係る発明は、上記の発明において、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記中継元情報が同一でないと判定された場合には、前記シグネチャの中継元である隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送し、さらに、当該既登録通知を他の隣接中継装置から受信した場合には、前記シグネチャ記憶手段に記憶された中継先情報から当該隣接中継装置に対応する中継先情報を削除することを特徴とする。

[0018] また、請求項11に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する複数の中継装置からなるネットワーク攻撃防御システムであって、前記中継装置は、前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手段と、前記攻撃有無判定手段によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手段と、を備えたことを特徴とする。

[0019] また、請求項12に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する複数の中継装置からなるネットワーク攻撃防御システムであって、前記中継装置は、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、を備えたことを特徴とする。

[0020] また、請求項13に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継

装置における中継方法であって、前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定工程と、前記攻撃有無判定工程によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信工程と、を含んだことを特徴とする。

[0021] また、請求項14に係る発明は、上記の発明において、前記攻撃有無判定工程は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定工程を含み、前記シグネチャ送信工程は、前記パケット数判定工程によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

[0022] また、請求項15に係る発明は、上記の発明において、前記攻撃有無判定工程は、前記パケット数判定工程によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定工程をさらに含み、前記シグネチャ送信工程は、前記連続超過回数判定工程によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

[0023] また、請求項16に係る発明は、上記の発明において、前記シグネチャ送信工程は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする。

[0024] また、請求項17に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継方法であって、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定工程と、前記識別情報判定工程によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグ

ネチャを他の隣接中継装置に送信するシグネチャ通信工程と、を含んだことを特徴とする。

[0025] また、請求項18に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、前記シグネチャ登録判定工程は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、前記シグネチャ通信工程は、前記シグネチャ登録判定工程によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする。

[0026] また、請求項19に係る発明は、上記の発明において、攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成工程を含み、当該シグネチャ生成工程は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする。

[0027] また、請求項20に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置としてのコンピュータに実行させる中継プログラムであって、前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手順と、前記攻撃有無判定手順によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手順と、をコンピュータに実行させることを特徴とする。

[0028] また、請求項21に係る発明は、上記の発明において、前記攻撃有無判定手順は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定手順をコンピュータに実

行させ、前記シグネチャ送信手順は、前記パケット数判定手順によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

[0029] また、請求項22に係る発明は、上記の発明において、前記攻撃有無判定手順は、前記パケット数判定手順によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定手順をさらにコンピュータに実行させ、前記シグネチャ送信手順は、前記連続超過回数判定手順によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

[0030] また、請求項23に係る発明は、上記の発明において、前記シグネチャ送信手順は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする。

[0031] また、請求項24に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置としてのコンピュータに実行させる中継プログラムであって、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手順と、前記識別情報判定手順によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手順と、をコンピュータに実行させることを特徴とする。

[0032] また、請求項25に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、前記シグネチャ登録判定手順は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、前記シグネチャ通信手順は、前記シグネチャ登録判定手順によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されてい

ないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする。

[0033] また、請求項26に係る発明は、上記の発明において、攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手順をコンピュータに実行させ、当該シグネチャ生成手順は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする。

発明の効果

[0034] 請求項1の発明によれば、隣接中継装置から受信したシグネチャに基づいて受信したシグネチャを他の隣接中継装置に送信すべきか否かを判定し、他の隣接中継装置に送信すべきと判定された場合に、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信するので、各中継装置によってシグネチャが重複送信されたり、ネットワーク上の全ての中継装置にシグネチャが送信されたりといった事態はなくなり、ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能になる。

[0035] 請求項2、11、13または20の発明によれば、隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して攻撃の有無を判定し、攻撃有りと判定した場合に初めてシグネチャを隣接中継装置に送信するので、ネットワーク上の全ての中継装置に容疑シグネチャが送信される事態はなくなり、ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能になる。

[0036] また、請求項3、14または21の発明によれば、隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過した場合に攻撃有りと判定するので、攻撃の有無を客観的かつ確実に判定することが可能になる。

[0037] また、請求項4、15または22の発明によれば、シグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過した場合に直ちに攻撃有りと判定するのでは

なく、所定の閾値を連続して超過した回数が所定値を超過した場合に初めて攻撃有りと判定するので、攻撃の有無をより確実に判定することが可能になる。

[0038] また、請求項5、16または23の発明によれば、自己にシグネチャを送信した隣接中継装置を除いた他の隣接中継装置にシグネチャを送信するので、既にパケットの規制に関する処理を行っている中継装置に対するシグネチャの送信が防止され、ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能になる。

[0039] また、請求項6、12、17または24の発明によれば、隣接中継装置から受信したシグネチャが既に登録されているか否かを判定して、未だ登録されていないシグネチャのみをシグネチャ記憶手段(シグネチャリスト)に登録するとともに隣接中継装置に送信するので、シグネチャの重複登録や重複送信が回避され、シグネチャに基づいたパケット制御を効率的に行うことが可能になる。

[0040] また、請求項7、18または25の発明によれば、シグネチャの生成を一意に識別するための生成識別情報(生成元である中継装置を一意に識別するための識別子および当該中継装置で生成される複数の容疑シグネチャをそれぞれ一意に識別するための識別子からなる生成識別情報)を各シグネチャに対応付けて管理するので、シグネチャの具体的な内容にまで踏み込むことなく、生成識別情報のみからシグネチャが既に登録されているか否かを判定することが可能になる。また、シグネチャの内容が同一であっても生成識別情報(生成元)が異なっていれば、未だ登録されていないシグネチャであるとしてシグネチャリストに登録するとともに隣接中継装置に送信するので、生成元となる各中継装置の性能違い(例えば、攻撃検出や防御解除に係るアルゴリズムの違いなど)が尊重され、安全性の高いパケット制御を行うことが可能になる。

[0041] また、請求項8、19または26の発明によれば、攻撃容疑パケットを検出すると、シグネチャおよび生成識別情報を生成し、これらシグネチャおよび生成識別情報を隣接中継装置に送信するとともに、中継先である隣接中継装置を特定するための中継先情報、生成識別情報およびシグネチャをシグネチャリストに対応付けて登録するので、シグネチャに対して確実に生成識別情報を付与することが可能になる。また、送信

ミスや内容更新等に起因してシグネチャを再送信する必要が生じた場合でも、シグネチャリストに登録された中継先情報、生成識別情報およびシグネチャを参照することで、同一の生成識別情報が付与されたシグネチャを同一の中継先に対して確実に再送信することが可能になる。

[0042] また、請求項9の発明によれば、隣接中継装置から受信したシグネチャの生成識別情報がシグネチャリストに未だ登録されていない場合には、これを他の隣接中継装置に送信するとともに、シグネチャの直前の中継元である隣接中継装置を特定するための中継元情報、シグネチャの直後の中継先である隣接中継装置を特定するための中継先情報、生成識別情報およびシグネチャをシグネチャリストに対応付けて登録する。そして、隣接中継装置から受信したシグネチャの生成識別情報がシグネチャリストに既に登録されている場合には、中継元情報が同一であるか否かをさらに判定し、これが同一である場合には、シグネチャをシグネチャリストに上書き登録するとともに、シグネチャリストに登録されている中継先情報が示す他の隣接中継装置にシグネチャを送信するので、送信ミスや内容更新等に起因してシグネチャが再送信されてきた場合でも、このシグネチャを留めることなく、中継先に対して確実に再送信することが可能になる。その一方、中継元情報が同一でない場合には、シグネチャの再送信でもないと判定される結果、シグネチャの重複登録や重複送信を確実に回避することが可能になる。

[0043] また、請求項10の発明によれば、隣接中継装置から受信したシグネチャの生成識別情報がシグネチャリストに既に登録されており、かつ、中継元情報も同一でない場合には、シグネチャの中継元である隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。さらに、当該既登録通知を他の隣接中継装置から受信した場合には、シグネチャリストに記憶された中継先情報から当該隣接中継装置に対応する中継先情報を削除する。したがって、送信ミスや内容更新等に起因してシグネチャを再送信する必要が生じた場合でも、シグネチャリストから削除された中継先に対してはシグネチャが送信されないことになり、シグネチャの再送信に際してもシグネチャの重複登録や重複送信を確実に回避することが可能になる。

図面の簡単な説明

[0044] [図1]図1は、実施例1に係るネットワーク攻撃防御システムの構成を示すシステム構成図である。

[図2]図2は、実施例1に係る中継装置の構成を示すブロック図である。

[図3]図3は、攻撃容疑検出条件テーブルに記憶される情報の例を示す図である。

[図4]図4は、不正トラヒック検出条件テーブルに記憶される情報の例を示す図である。

[図5]図5は、正規条件テーブルに記憶される情報の例を示す図である。

[図6]図6は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。

[図7]図7は、シグネチャ受信時の処理手順を示すフローチャートである。

[図8]図8は、不正パケット検出時の処理手順を示すフローチャートである。

[図9]図9は、パケット制御時の処理手順を示すフローチャートである。

[図10]図10は、実施例2に係るネットワーク攻撃防御システムの構成を示すシステム構成図である。

[図11]図11は、実施例2に係る中継装置の構成を示すブロック図である。

[図12]図12は、攻撃容疑検出条件テーブルに記憶される情報の例を示す図である。

[図13]図13は、不正トラヒック検出条件テーブルに記憶される情報の例を示す図である。

[図14]図14は、正規条件テーブルに記憶される情報の例を示す図である。

[図15]図15は、シグネチャリストに記憶される情報の例を示す図である。

[図16]図16は、シグネチャに付与される識別情報の例を示す図である。

[図17]図17は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。

[図18]図18は、シグネチャ受信時の処理手順を示すフローチャートである。

[図19]図19は、不正パケット検出時の処理手順を示すフローチャートである。

[図20]図20は、パケット制御時の処理手順を示すフローチャートである。

[図21]図21は、実施例3に係る中継装置の構成を示すブロック図である。

[図22]図22は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。

[図23]図23は、シグネチャ受信時の処理手順を示すフローチャートである。

[図24]図24は、従来技術に係るネットワーク攻撃防御システムを説明するための図である。

[図25]図25は、従来技術に係るネットワーク攻撃防御システムを説明するための図である。

符号の説明

[0045] 10 中継装置

11 ネットワークインタフェース

12 パケット取得部

13 攻撃検出部

14 シグネチャ通信部(シグネチャ送信部)

15a、215b パケット数判定部

15b、215c 連続超過回数判定部

16 フィルタ部

20 サーバ

30 通信端末

100、100a ネットワーク攻撃防御システム

110 中継装置

111 ネットワークインタフェース

112 パケット取得部

113 攻撃検出部

114 シグネチャ通信部

115、215a 識別情報判定部

116 フィルタ部

120 サーバ

130 通信端末

発明を実施するための最良の形態

[0046] 以下に添付図面を参照して、この発明に係る中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムの実施例を詳細に説明する。なお、実施

例1では、所定の閾値を用いてシグネチャの転送処理を制限する場合について、実施例2では、シグネチャの生成識別情報を用いてシグネチャの転送処理を制限する場合についてそれぞれ説明する。また、実施例3では、実施例1および実施例2で行うパケット制限処理を組み合わせた場合について説明することとする。

[0047] 各実施例の説明に先立って、この発明に係る中継方式の概要について説明する。本発明に係る中継方式では、隣接する中継装置から受信したシグネチャをそのまま他の中継装置に転送するのではなく、受信したシグネチャを転送すべきか否かを判定したうえで、転送すべきと判定した場合にのみ他の隣接する中継装置に転送する点に主たる特徴がある。

[0048] たとえば、単位時間内のパケット数が所定の閾値を超過した場合や、所定の閾値を連続して超過した回数が所定値を超過した場合にのみ、受信したシグネチャを他の中継装置に転送することとする。また、シグネチャの生成を一意に識別するための生成識別情報を各シグネチャに対応付けて管理し、この生成識別情報が所定の条件を満たした場合にのみ、受信したシグネチャを他の中継装置に転送する。

[0049] このようにすることで、各中継装置によってシグネチャが重複送信されたり、ネットワーク上の全ての中継装置にシグネチャが送信されたりといった事態はなくなり、ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能になる。

実施例 1

[0050] 実施例1では、所定の閾値を用いてシグネチャの転送処理を制限する場合について説明する。なお、以下では、本実施例1で用いる主要な用語、ネットワーク攻撃防御システムの概要および特徴、中継装置の構成および処理、本実施例1の効果を順に説明し、最後に本実施例1に対する種々の変形例を説明する。

[0051] [用語の説明]

まず最初に、本実施例1で用いる主要な用語を説明する。本実施例1で用いる「容疑シグネチャ」とは、攻撃容疑のあるパケット(攻撃容疑パケット)を制限するためのシグネチャであり、具体的には、通過が制限される攻撃容疑パケットの特徴を示す属性(例えば、宛先IPアドレス、プロトコル、宛先ポート番号など)や制限内容(例えば、特

定のパケットが流入するときの帯域を制限するための制限情報など）を規定して構成される。

[0052] また、本実施例1で用いる「正規シグネチャ」とは、容疑シグネチャに該当するパケットのなかから攻撃とはみなされない正規パケット（正規ユーザの通信パケットである正規パケット）の通過を許可するためのシグネチャであり、具体的には、通過が許可される正規パケットの特徴を示す属性（例えば、送信元IPアドレス、サービスタイプ、宛先IPアドレス、プロトコル、宛先ポート番号など）を規定して構成される。

[0053] また、本実施例1で用いる「不正シグネチャ」とは、不正トラヒックに含まれる不正パケット（不正トラヒック条件を満たすパケット）を制限するためのシグネチャであり、具体的には、不正パケットの送信元IPアドレス等を規定して構成される。

[0054] ［システムの概要および特徴］

次に、図1を用いて、本実施例1に係るネットワーク攻撃防御システムの概要および特徴を説明する。図1は、本実施例1に係るネットワーク攻撃防御システムの構成を示すシステム構成図である。

[0055] 同図に示すように、このネットワーク攻撃防御システム100は、ネットワーク上に複数の中継装置10を備えて構成される。また、このネットワーク上には、DoS攻撃やDDoS攻撃の対象となるコンピュータとしてのサーバ20や、かかるDoS攻撃やDDoS攻撃を行い得るコンピュータとしての通信端末30が接続されている。なお、以下では、図示した中継装置10の各々を区別する場合には、それぞれ中継装置10－1～中継装置10－7として説明し、サーバ20の各々を区別する場合には、サーバ20－1またはサーバ20－2として説明し、通信端末30の各々を区別する場合には、通信端末30－1～通信端末30－5として説明する。

[0056] かかるネットワーク攻撃防御システム100において、中継装置10は、通信端末30のうち少なくとも1つ以上の通信端末30がネットワーク上のサーバ20に対してDoS攻撃またはDDoS攻撃を行っていることを検出した場合に、パケットの通過を制御するためのシグネチャ（容疑シグネチャや不正シグネチャ）を生成するとともに、パケットの通過を許可するための正規シグネチャを生成する。そして、中継装置10は、自ら生成したシグネチャ（容疑シグネチャ、不正シグネチャおよび正規シグネチャ）をシグネ

チャリストに登録する。

[0057] また、中継装置10は、生成した容疑シグネチャ(さらには、正規シグネチャの生成に用いた正規条件)を隣接中継装置に送信する。その一方で、中継装置10は、隣接中継装置から容疑シグネチャ等を受信した場合には、正規条件に基づいて正規シグネチャを生成するとともに、受信した容疑シグネチャおよび生成した正規シグネチャをシグネチャリストに登録し、さらに、隣接中継装置から受信したシグネチャ等を他の隣接中継装置に送信する。なお、隣接中継装置について例を挙げると、図1において、中継装置10－3における隣接中継装置は、中継装置10－1、中継装置10－2、中継装置10－4および中継装置10－7であり、中継装置10－5および中継装置10－6とは、隣接関係をもたない。また、この隣接関係は、物理的な隣接を意味するものではない。

[0058] そして、中継装置10は、上記のようにしてシグネチャリストに登録されたシグネチャに基づいてパケットの通過を制御する。つまり、不正シグネチャや容疑シグネチャに該当するパケットについては、伝送帯域を制限して通過させるかもしくは廃棄し、正規シグネチャに該当するパケットやいずれのシグネチャにも該当しないパケットについては、伝送帯域を制限せずに通過を許可する。

[0059] なお、中継装置10は、攻撃を防御しながらパケットを中継するための装置であり、例えば、ルータとして機能してもよく、または、ブリッジとして機能してもよい。また、中継装置10は、中継装置10等を管理するための管理用ネットワークに接続されていてもよく、シグネチャは、管理用ネットワークを介して送受されてもよい。

[0060] このように、中継装置10は、パケットの通過を制御するためのシグネチャ等を自ら生成してパケットを制御するだけでなく、生成したシグネチャを隣接中継装置に送信する。さらに、中継装置10は、隣接中継装置からシグネチャを受信した場合には、かかるシグネチャに基づいてパケットを制御するとともに、他の隣接中継装置にもシグネチャを送信する。そして、本実施例1における中継装置10は、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理に主たる特徴があり、隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して攻撃の有無を判定し、攻撃有りと判定した場合に初めてシグネチャを隣接中継装置に送信するように

している。

[0061] この主たる特徴について図1を用いて簡単に説明する。図1に示すように、例えば、通信端末30－4および通信端末30－5がサーバ20－1に対するDoS攻撃を行っており、中継装置10－1が容疑のかかる攻撃を検出したとすると、中継装置10－1は、攻撃容疑パケットを制限するための容疑シグネチャを生成し、生成した容疑シグネチャに基づいてパケットを処理するとともに、容疑シグネチャ（さらには正規条件）を隣接中継装置となる中継装置10－3に送信する（図1の（1）および（2）参照）。

[0062] 一方、中継装置10－3は、中継装置10－1から送信された容疑シグネチャを受信し、受信した容疑シグネチャに基づいてパケットを処理するとともに、受信した容疑シグネチャの条件を満たすパケットの数が単位時間内に所定の閾値を超過したか否かを判定する（図1の（3）参照）。すなわち、かかる容疑シグネチャに該当する攻撃が中継装置10－3を経由して行われているか否か、攻撃の有無を判定する。

[0063] そして、かかる判定において、容疑シグネチャの条件を満たすパケットの数が単位時間内に所定の閾値を超過した場合には、中継装置10－3は、中継装置10－1から受信した容疑シグネチャを隣接中継装置に送信する（図1の（4）参照）。ここで、中継装置10－3が容疑シグネチャを送信する隣接中継装置は、容疑シグネチャを自己（中継装置10－3）に送信した隣接中継装置（中継装置10－1）を除く隣接中継装置、すなわち、中継装置10－2、中継装置10－4および中継装置10－7である。また、図1に示す例では、通信端末30－4および通信端末30－5がサーバ20－1に対する攻撃を行っているので、中継装置10－3では「攻撃有り」と判定される。

[0064] さらに、中継装置10－4および中継装置10－2は、中継装置10－3から送信された容疑シグネチャを受信し、受信した容疑シグネチャに基づいてパケットを処理するとともに、上記と同様、かかる容疑シグネチャに該当する攻撃が各中継装置を経由して行われているか否か判定する（図1の（5）および（6）参照）。ここで、図1に示す例では、通信端末30－4および通信端末30－5がサーバ20－1に対する攻撃を行っているので、中継装置10－2および中継装置10－4では、受信した容疑シグネチャの条件を満たすパケットの数が単位時間内に所定の閾値を超過したと判定されず（つまり「攻撃無し」と判定され）、その結果、容疑シグネチャを隣接中継装置に送信す

ることはしない。

[0065] 一方、中継装置10－7は、上記した中継装置10－4および中継装置10－2と同様、中継装置10－3から送信された容疑シグネチャを受信し、受信した容疑シグネチャに基づいてパケットを処理するとともに、かかる容疑シグネチャに該当する攻撃が各中継装置を経由して行われているか否か判定するが、容疑シグネチャを自己に送信した隣接中継装置を除く隣接中継装置が存在しないため、容疑シグネチャを隣接中継装置に送信することはしない(図1の(7)参照)。

[0066] 以上のように、ネットワーク攻撃防御システム100において、複数の中継装置10のうち、中継装置10－1、中継装置10－3および中継装置10－7が、通信端末30－4および通信端末30－5から送信されるパケットを容疑シグネチャに基づいて制限しながら中継する。言い換えれば、ネットワーク攻撃防御システム100の中継装置10のうち、中継装置10－5および中継装置10－6には容疑シグネチャが送信されない(全ての中継装置10に容疑シグネチャが送信されるわけではない)。このため、容疑のかかる攻撃を検出したとき等の各中継装置10にかかる処理負荷を低減することが可能になる。

[0067] なお、中継装置10が送信するシグネチャは、容疑シグネチャだけに限定されず、中継装置10が他のシグネチャを送信するようにしてもよく、また、容疑シグネチャに加えて他のシグネチャを送信するようにしてもよい。

[0068] [中継装置の構成]

次に、図2を用いて、図1に示した中継装置10の構成を説明する。図2は、中継装置10の構成を示すブロック図である。同図に示すように、この中継装置10は、ネットワークインタフェース部11と、パケット取得部12と、攻撃検出部13(並びに攻撃容疑検出条件テーブル13a、不正トラヒック検出条件テーブル13bおよび正規条件テーブル13c)と、シグネチャ通信部14と、パケット数判定部15aと、連続超過回数判定部15bと、フィルタ部16(並びにシグネチャリスト16a)とを備えて構成される。

[0069] また、中継装置10は、CPU(CentralProcessingUnit)やメモリ、ハードディスク等を有しており、パケット取得部12、攻撃検出部13、シグネチャ通信部14、パケット数判定部15a、連続超過回数判定部15bおよびフィルタ部16は、CPUによって処理され

るプログラムのモジュールであってもよい。また、このプログラムのモジュールは、1つのCPUで処理されてもよく、複数のCPUに分散して処理されてもよい。さらに、中継装置10には、Linux等の汎用OSをインストールしておき、汎用OSに具備されるパケットフィルタをフィルタ部16として機能させてもよい。

[0070] なお、シグネチャ通信部14は特許請求の範囲に記載の「シグネチャ送信手段」に対応し、パケット数判定部15aは同じく「攻撃有無判定手段」および「パケット数判定手段」に対応し、連続超過回数判定部15bは同じく「攻撃有無判定手段」および「連続超過回数判定」に対応する。

[0071] 図2において、ネットワークインタフェース部11は、ネットワークと接続されている通信機器との間でパケットを送受する手段であり、具体的には、LAN(LocalAreaNetwork)またはWAN(WideAreaNetwork)などのネットワークと接続するためのネットワーク接続カード等によって構成される。なお、図2には示していないが、キーボードやマウス、マイクなど、ネットワーク管理者から各種の情報や指示の入力を受付ける入力手段や、モニタ(若しくはディスプレイ、タッチパネル)やスピーカなど、各種の情報を出力する出力手段を備えて中継装置10を構成するようにしてもよい。

[0072] パケット取得部12は、ネットワークインタフェース部11が受信したパケットを取得し、取得したパケットの統計に関する統計情報を攻撃検出部13およびパケット数判定部15aに提供する処理部である。

[0073] 攻撃検出部13は、パケット取得部12によって提供された統計情報に基づいて、攻撃の検出および攻撃の分析を行う処理部であり、図2に図示するように、攻撃容疑検出条件テーブル13a、不正トラヒック検出条件テーブル13bおよび正規条件テーブル13cにそれぞれ接続される。ここで、各テーブル13a～13cに記憶される情報を具体的に説明した後に、攻撃検出部13による処理内容を説明する。

[0074] 図3は、攻撃容疑検出条件テーブル13aに記憶される情報、より詳細には、受信パケットが攻撃パケットである可能性がある攻撃容疑パケットを検出するために使用される「攻撃容疑検出条件」の一例を示す図である。同図に示すように、攻撃容疑検出条件は、検出属性、検出閾値および検出間隔の組合せからなる複数組(ここでは3組)のレコードで構成され、かかる攻撃容疑検出条件の各レコードの内のいずれかのレコ

ードの条件にトラヒックが一致した場合に、このトラヒックの通信パケットは攻撃容疑パケットであると認識される。なお、番号はレコードを特定するために便宜上使用されるものである。

[0075] 攻撃容疑検出条件の「検出属性」には、例えば、IPパケットに含まれるIPヘッダ部の属性や、IPパケットのペイロード部に含まれるTCPヘッダ部またはUDPヘッダ部の属性が指定される。具体的には、図3において、番号1のレコードの検出属性は、「DestinationIPAddress(宛先IPアドレス)」が「192.168.1.1/32」であり(dst=192.168.1.1/32)、IPの上位層(TCPまたはUDP)のプロトコル種別を示す「Protocol(プロトコル)」が「TCP」であり(Protocol=TCP)、かつ、IPの上位層プロトコルがどのアプリケーションの情報であるかを示す「DestinationPort(宛先ポート番号)」が「80」である(Port=80)という属性値の組で指定される。

[0076] また、番号2のレコード検出属性は、「DestinationIPAddress(宛先IPアドレス)」が「192.168.1.2/32」であり(dst=192.168.1.2/32)、かつ、「Protocol(プロトコル)」が「UDP(UserDatagramprotocol)」である(Protocol=UDP)という属性値の組で指定される。同様に、番号3のレコード検出属性は、「DestinationIPAddress(宛先IPアドレス)」が「192.168.1.0/24」という属性で指定される。

[0077] 攻撃容疑検出条件の「検出閾値」は、同じレコードで指定される検出属性を持つ受信パケットのトラヒックを攻撃容疑トラヒックとして検出するための最低の伝送帯域を指定したものであり、攻撃容疑検出条件の「検出間隔」は、同じく最低の連続時間を指定したものである。なお、図3には示していないが、検出属性においては、「DestinationIPAddress(宛先IPアドレス)」の値を無条件(any)とし、かつ、IPの上位層のプロトコル種別を示す「Protocol(プロトコル)」が「ICMP(InternetControlMessageProtocol)」となる属性値の組を指定するようにしてもよい。

[0078] 図4は、不正トラヒック検出条件テーブル13bに記憶される情報、より詳細には、攻撃容疑パケットのトラヒックから不正トラヒックを検出するために用いられる「不正トラヒック条件」の一例を示す図である。同図に示すように、不正トラヒック条件は、既知のDDoS攻撃の複数のトラヒックパターンから構成され、攻撃容疑パケットのトラヒックがいずれかのトラヒックパターンに合致した場合に、不正トラヒックであると認識される。な

お、番号はレコード(パターン)を特定するために便宜上使用されるものである。

[0079] 具体的には、番号1の不正トラヒック条件は、「伝送帯域T1Kbps以上、パケットがS1秒以上連続送信されている」というトラヒックパターンを示している。また、番号2の不正トラヒック条件は、「伝送帯域T2Kbps以上、ICMP(InternetControlMessageProtocol)上のエコー応答(EchoReply)メッセージのパケットがS2秒以上連続送信されている」というトラヒックパターンを示している。さらに、番号3の不正トラヒック条件は、「伝送帯域T3Kbps以上、データが長すぎるためパケットに含まれるデータは複数IPパケットに分割して送信していることを示すフラグメントパケットがS3秒以上連続送信されている」というトラヒックパターンを示している。

[0080] 図5は、正規条件テーブル13cに記憶される情報、より詳細には、正当な利用者が利用している通信端末30から送信されるパケットを表す「正規条件」の一例を示す図である。同図に示すように、正規条件は、IPパケットにおける属性とそれら属性値の組からなる複数のレコードで構成される。なお、番号はレコード(パターン)を特定するために便宜上使用されるものである。

[0081] 具体的には、番号1のレコードの検出属性は、IPの「SourceIPAddress(送信元IPアドレス)」が「172.16.10.0/24」であることを指定し(src=172.16.10.0/24)、番号2のレコードの検出属性はIP上のサービス品質を示す「TypeofService(サービスタイプ)」が「(16進で)01」であることを指定している(TOS=0x01)。このような正規条件には、例えば、サーバ所有者の会社の支店や、関連会社など、防御対象のサーバ20等の送信元IPアドレスが設定され、サーバ20が収容されているLANの所有者が正規ユーザであると認識しているネットワークの送信元IPアドレスなどが設定される。

[0082] 図2の説明に戻ると、攻撃検出部13は、パケット取得部12によって提供された統計情報に基づいて攻撃の検出を検出した場合に、攻撃容疑トラヒックの通信パケット(攻撃容疑パケット)を制限するための容疑シグネチャを生成する。具体的には、攻撃検出部13は、図3に示した攻撃容疑検出条件に従って、検出間隔で指定されているより長い時間連続して、検出閾値で指定されている以上の伝送帯域を使用している、検出属性に合致するトラヒックをチェックし、各レコードの内のいずれかのレコードに合致した場合には、このトラヒックを攻撃容疑トラヒックとして検出し、このときに検出さ

れた攻撃容疑トラヒックが満たしている攻撃容疑検出条件のレコードの検出属性を容疑シグネチャとして生成する。

[0083] また、攻撃検出部13は、攻撃を検出した場合に、容疑シグネチャとともに正規シグネチャを生成する。具体的には、図5に示した正規条件を参照し、正規条件の全てのレコード毎に、容疑シグネチャとのAND条件をとり、これを正規シグネチャとして生成する。この正規シグネチャは、容疑シグネチャから正規ユーザの通信パケットである正規パケットを許可するために用いられるシグネチャであるが、例えば、図3および図5の例を用いて説明すると、図3における番号1のレコードの条件で検出されるパケットの容疑シグネチャは、[dst=192.168.1.1/32,Protocol=TCP,Port=80]となり、図5において、正規シグネチャは、[src=172.16.10.24,dst=192.168.1.1/32,Protocol=TCP,Port=80]および[TOS=0x01,dst=192.168.1.1/32,Protocol=TCP,Port=80]となる。

[0084] さらに、攻撃検出部13は、図4に示した不正トラヒック条件のいずれかのパターンに合致するトラヒックを検出した場合に、不正トラヒックを制限するための不正シグネチャを生成する。具体的には、検出された不正トラヒック条件を満たすパケットの送信元IPアドレスを不正アドレス範囲として特定し、この不正アドレス範囲であり、かつ、容疑シグネチャに合致するという条件を不正シグネチャとして生成する。

[0085] 上述してきた攻撃検出部13によって生成された容疑シグネチャ、正規シグネチャおよび不正シグネチャは、シグネチャリスト16aに登録される。なお、シグネチャリスト16aに登録されるシグネチャ(容疑シグネチャ、正規シグネチャおよび不正シグネチャ)としては、かかる攻撃検出部13によって生成されたシグネチャの他に、後述するシグネチャ通信部14を介して隣接中継装置から受信したシグネチャもある。

[0086] 図2において、シグネチャ通信部14は、攻撃検出部13が生成したシグネチャ等を隣接中継装置に送信するとともに、隣接中継装置から送信されたシグネチャを受信し、さらに、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理部である。ここで、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理は、後述するパケット数判定部15aおよび連続超過回数判定部15bによる判定結果に従って実行される。

[0087] パケット数判定部15aは、シグネチャ通信部14によって受信されたシグネチャの条

件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定する処理部である。具体的には、パケット数判定部15aは、パケット取得部12によって提供された統計情報から、シグネチャの条件を満たすパケットを単位時間毎に取得し、取得したパケットの数が所定の閾値を超過したか否かを判定する。

[0088] 連続超過回数判定部15bは、パケット数判定部15aが所定の閾値を超過したと判定した場合に、所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する処理部である。そして、連続超過回数判定部15bは、所定の閾値を連続して超過した回数が所定値を超過した場合には、シグネチャ送信部14に対して、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信するように指示を出力する。なお、かかる指示を受けたシグネチャ送信部14は、シグネチャを自己に送信した隣接中継装置を除く隣接中継装置を選択し、選択した隣接中継装置に対してシグネチャを送信する。

[0089] 図2において、フィルタ部16は、ネットワークインタフェース部11が受信したパケットを受け入れて、シグネチャリスト16aに基づいてパケットの通過(ネットワークインタフェース部11からのパケットの出力)を制御する処理部である。具体的には、入力されたパケットについて、シグネチャリスト16aに登録された「不正シグネチャ」、「正規シグネチャ」、「容疑シグネチャ」のいずれかに該当するか(もしくはいずれにも該当しないか)を判別した上で、該当するシグネチャに基づいてパケットの通過を制御する。

[0090] より詳細には、フィルタ部16は、不正シグネチャに該当するパケットは、不正なパケットを処理するための不正キューに入力し、容疑シグネチャに該当するパケットは、容疑ユーザ用の容疑キューに入力し、正規シグネチャに該当するパケットまたはいずれのシグネチャにも該当しないパケットは、正規ユーザ用の正規キューに入力する。その上で、フィルタ部16は、正規キューに入力されたパケットについては、伝送帯域を制限せずにネットワークインタフェース部11から出力し、容疑キューおよび不正キューに入力されたパケットについては、それぞれのシグネチャ(条件を満たすとして選択されたシグネチャ)が示す伝送帯域制限値に従って制限して出力する。

[0091] なお、フィルタ部16は、シグネチャリスト16aに登録されたシグネチャの検出属性等が所定の解除判断基準を満たした場合には、この所定の解除判断基準を満たしたシ

グネチャを解除し、解除したシグネチャに基づいてパケットの通過を制御する処理を停止する。

[0092] [攻撃容疑パケット検出時の処理]

続いて、図6を参照して、上記した中継装置10による攻撃容疑パケット検出時の動作処理を説明する。図6は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。

[0093] 同図に示すように、中継装置10の攻撃検出部13は、図3に示した攻撃容疑検出条件テーブル13aに基づいて攻撃容疑トラヒックを検出すると(ステップS1)、容疑シグネチャおよび正規シグネチャを生成する(ステップS2)。

[0094] そして、攻撃検出部13は、生成した容疑シグネチャおよび正規シグネチャをフィルタ部16のシグネチャリスト16aに登録する(ステップS3)。さらに、シグネチャ通信部14は、攻撃検出部13が生成したシグネチャ等(本実施例1では、容疑シグネチャおよび正規条件)を隣接中継装置に送信する(ステップS4)。

[0095] [シグネチャ受信時の処理]

続いて、図7を参照して、上記した中継装置10によるシグネチャ受信時の動作処理を説明する。図7は、シグネチャ受信時の処理手順を示すフローチャートである。

[0096] 同図に示すように、中継装置10のシグネチャ通信部14が、隣接中継装置から送信されたシグネチャ等(本実施例1では、容疑シグネチャおよび正規条件)を受信すると(ステップS11)、攻撃検出部13は、シグネチャ通信部14が受信した正規条件に基づいて正規シグネチャを生成する(ステップS12)。

[0097] さらに、攻撃検出部13は、隣接中継装置から受信した容疑シグネチャおよび上記で生成した正規シグネチャをフィルタ部16のシグネチャリスト16aに登録する(ステップS13)。その後、パケット数判定部15aは、パケット取得部12によって提供された統計情報から、上記でシグネチャリスト16aに登録した容疑シグネチャの条件を満たすパケットを単位時間毎に取得し、取得したパケットの数が所定の閾値を超過したか否かを判定する(ステップS14)。

[0098] ここで、かかる所定の閾値を超過した場合(ステップS14肯定)、連続超過回数判定部15bは、所定の閾値を連続して超過した回数が、所定値を超過したか否かを判定

する（ステップS15）。その結果、かかる所定の閾値を連続して超過した回数が所定値を超過した場合（ステップS15肯定）、シグネチャ送信部14は、上記で受信した容疑シグネチャおよび正規条件を隣接中継装置に送信する（ステップS16）。つまり、シグネチャを自己に送信した隣接中継装置を除く隣接中継装置を選択し、選択した隣接中継装置に対してシグネチャを送信する。

[0099] なお、上記したステップS14において、パケットの数が所定の閾値を超過しなかった場合（ステップS14否定）や、上記したステップS15において、所定の閾値を連続して超過した回数が所定値を超過しなかった場合（ステップS15否定）には、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理（上記のステップS16の処理）は行われない。

[0100] ［不正パケット検出時の処理］

続いて、図8を参照して、上記した中継装置10による不正パケット検出時の動作処理を説明する。図8は、不正パケット検出時の処理手順を示すフローチャートである。

[0101] 同図に示すように、中継装置10の攻撃検出部13が、図4に示した不正トラヒック条件検出テーブル13b等に基づいて不正トラヒックを検出すると（ステップS21）、不正シグネチャを生成する（ステップS22）。そして、攻撃検出部13は、生成した不正シグネチャをフィルタ部16のシグネチャリスト16aに登録する（ステップS23）。

[0102] ［パケット制御時の処理］

続いて、図9を参照して、上記した中継装置10によるパケット制御時の動作処理を説明する。図9は、パケット制御時の処理手順を示すフローチャートである。

[0103] 同図に示すように、フィルタ部16は、ネットワークインタフェース部11からパケットが入力されると、シグネチャリスト16aに登録された不正シグネチャに合致するか否かを判断する（ステップS31）。そして、不正シグネチャに合致した場合には（ステップS31肯定）、フィルタ部16は、不正なパケットを処理するための不正キューにパケットを入力する（ステップS32）。

[0104] これとは反対に、不正シグネチャに合致しない場合には（ステップS31否定）、フィルタ部16は、入力されたパケットが、シグネチャリスト16aに登録された正規シグネチャに合致するか否かを判断する（ステップS33）。そして、正規シグネチャに合致した

場合には(ステップS33肯定)、フィルタ部16は、正規なユーザ用の正規キューにパケットを入力する(ステップS34)。

[0105] さらに、この正規シグネチャにも合致しない場合には(ステップS33否定)、フィルタ部16は、入力されたパケットが、シグネチャリスト16aに登録された容疑シグネチャに合致するか否かを判断する(ステップS35)。そして、容疑シグネチャに合致した場合には(ステップS35肯定)、フィルタ部16は、容疑ユーザ用の容疑キューにパケットを入力する(ステップS36)。これとは反対に、容疑シグネチャに合致しない場合には(ステップS35否定)、フィルタ部16は、正規キューにパケットを入力する(ステップS37)。

[0106] そして、フィルタ部16は、それぞれのキューにあるパケットについて、正規キューであれば、伝送帯域を制限せずにネットワークインタフェース部11から出力し、容疑キューおよび不正キューであれば、それぞれのシグネチャが示す伝送帯域制限値に従って制限して出力する。なお、不正シグネチャ、正規シグネチャ、容疑シグネチャの各シグネチャは、それぞれシグネチャリスト16aに複数登録されてもよい。また、登録されたシグネチャの検出属性等が所定の判断基準を満たした場合に、フィルタ部16は、所定の判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいたパケットの通過を制御する処理を停止する。

[0107] [実施例1の効果]

上述してきたように、上記の実施例1によれば、隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して攻撃の有無を判定し、攻撃有りと判定した場合に初めてシグネチャを隣接中継装置に送信するので、ネットワーク上の全ての中継装置10に容疑シグネチャが送信される事態はなくなり、ネットワーク上にある各中継装置10の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能になる。

[0108] また、上記の実施例1によれば、隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過した場合に攻撃有りと判定するので、攻撃の有無を客観的かつ確実に判定することが可能になる。より詳細には、シグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過した場合に直ち

に攻撃有りと判定するのではなく、所定の閾値を連続して超過した回数が所定値を超過した場合に初めて攻撃有りと判定するので、攻撃の有無をより確実に判定することが可能になる。

[0109] また、上記の実施例1によれば、自己にシグネチャを送信した隣接中継装置を除いた他の隣接中継装置にシグネチャを送信するので、既にパケットの規制に関する処理を行っている中継装置10に対するシグネチャの送信が防止され、ネットワーク上にある各中継装置10の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能になる。

[0110] [他の実施例]

さて、これまで本発明の実施例1について説明したが、本発明は上述した実施例1以外にも、種々の異なる形態にて実施されてよいものである。

[0111] 例えば、上記の実施例1では、シグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過し、かつ、所定の閾値を連続して超過した回数が所定値を超過した場合に攻撃有りと判定する場合を説明したが、本発明はこれに限定されるものではなく、単位時間内のパケット数が所定の閾値を超過した場合に直ちに攻撃有りと判定するようにしてもよい。すなわち、上記の実施例1で説明した攻撃有無の判定手法は、あくまでも一例であって、本発明はこれに限定されるものではなく、他の攻撃有無判定手法を採用する場合にも本発明を同様に適用することができる。

[0112] また、上記の実施例1で図示した各装置(例えば、図1に例示した中継装置10)の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、中継装置10の分散・統合の具体的形態は図示のものに限られず、中継装置10の全部または一部を各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、中継装置10にて行なわれる各処理機能は、その全部または任意の一部が、CPUおよび当該CPUにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

[0113] また、上記の実施例1で説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的にお

こなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報（例えば、攻撃容疑検出条件テーブル、不正トラヒック検出条件テーブル、正規条件テーブルの内容等）については、特記する場合を除いて任意に変更することができる。

[0114] なお、上記の実施例1では、本発明を実現する各装置（例えば、中継装置10）を機能面から説明したが、各装置の各機能はパーソナルコンピュータやワークステーションなどのコンピュータにプログラムを実行させることによって実現することもできる。すなわち、本実施例1で説明した各種の処理手順は、あらかじめ用意されたプログラムをコンピュータ上で実行することによって実現することができる。そして、これらのプログラムは、インターネットなどのネットワークを介して配布することができる。さらに、これらのプログラムは、ハードディスク、フレキシブルディスク（FD）、CD－ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。つまり、例を挙げれば、実施例1に示したような中継装置用プログラムを格納したCD－ROMを配布し、このCD－ROMに格納されたプログラムを各コンピュータが読み出して実行するようにしてもよい。

実施例 2

[0115] 実施例2では、シグネチャの生成識別情報を用いてシグネチャの転送処理を制限する場合について説明する。なお、以下では、本実施例2で用いる主要な用語、従来技術の問題点、ネットワーク攻撃防御システムの概要および特徴、中継装置の構成および処理、本実施例2の効果を順に説明し、最後に本実施例2に対する種々の変形例を説明する。

[0116] ［用語の説明］

まず最初に、本実施例2で用いる主要な用語を説明する。本実施例2で用いる「容疑シグネチャ」とは、攻撃容疑のあるパケット（攻撃容疑パケット）を制限するためのシグネチャであり、具体的には、通過が制限される攻撃容疑パケットの特徴を示す属性（例えば、宛先IPアドレス、プロトコル、宛先ポート番号など）や制限内容（例えば、特

定のパケットが流入するときの帯域を制限するための制限情報など）を規定して構成される。

[0117] また、本実施例2で用いる「正規シグネチャ」とは、容疑シグネチャに該当するパケットのなかから攻撃とはみなされない正規パケット（正規ユーザの通信パケットである正規パケット）の通過を許可するためのシグネチャであり、具体的には、通過が許可される正規パケットの特徴を示す属性（例えば、送信元IPアドレス、サービスタイプ、宛先IPアドレス、プロトコル、宛先ポート番号など）を規定して構成される。

[0118] また、本実施例2で用いる「不正シグネチャ」とは、不正トラヒックに含まれる不正パケット（不正トラヒック条件を満たすパケット）を制限するためのシグネチャであり、具体的には、不正パケットの送信元IPアドレス等を規定して構成される。

[0119] また、本実施例2で用いる「識別情報（特許請求の範囲に記載の「生成識別情報」に対応する）」とは、上記したシグネチャの生成を一意に識別するための情報であり、具体的には、シグネチャの生成元である中継装置を一意に識別するための識別子（例えば、エンジンタイプ、エンジンIDおよびノードIDからなる識別子）および当該中継装置で生成される複数の容疑シグネチャをそれぞれ一意に識別するための識別子（例えば、シーケンシャルに付与される生成番号）から構成される。

[0120] また、本実施例2で用いる「下流ノード（特許請求の範囲に記載の「中継元情報」に対応する）」とは、上記したシグネチャを隣接する中継装置から受信して他の隣接する中継装置に送信した中継装置において、当該シグネチャの直前の中継元である隣接中継装置（すなわち、どの中継装置からシグネチャを受信したか）を特定するための情報であり、具体的には、隣接中継装置のアドレスを規定して構成される。

[0121] また、本実施例2で用いる「上流ノード（特許請求の範囲に記載の「中継先情報」に対応する）」とは、上記したシグネチャを隣接する中継装置から受信して他の隣接する中継装置に送信した中継装置において、当該シグネチャの直後の中継先である隣接中継装置（すなわち、どの中継装置に対してシグネチャを送信したか）を特定するための情報であり、具体的には、隣接中継装置のアドレスを規定して構成される。なお、シグネチャの中継元（下流ノード）は常に一つであるが、中継先（上流ノード）は複数になり得る。

[0122] ［従来技術の問題点］

ところで、従来の技術では、隣接中継装置にシグネチャを送信するので、ネットワーク攻撃防御システムにおける互いの中継装置の隣接関係によっては、異なる隣接中継装置から同一のシグネチャを受信する中継装置が存在することがある。そして、このような中継装置では、重複したシグネチャに基づいた処理を行う結果、シグネチャに基づいたパケットの規制に関する処理を効率的に行うことができないという問題がある。以下に、図24および図25を用いて、この問題を具体的に説明する。図24および図25は、従来技術に係るネットワーク攻撃防御システムを説明するための図である。

[0123] 図24に示すように、中継装置109－1は、2つの通信端末130がネットワーク上のサーバ120に対するDDoS攻撃を行っていることを検出すると（同図の（1）参照）、シグネチャを隣接中継装置となる中継装置109－2および中継装置109－3に送信する（同図の（2）参照）。そして、隣接中継装置となる中継装置109－1からシグネチャを受信した中継装置109－2は、受信したシグネチャに基づいてパケットを処理するとともに、シグネチャを隣接中継装置となる中継装置109－3に送信する。同様に、隣接中継装置となる中継装置109－1からシグネチャを受信した中継装置109－3は、受信したシグネチャに基づいてパケットを処理するとともに、シグネチャを隣接中継装置となる中継装置109－2に送信する（同図の（3）参照）。なお、図24に示す例では、隣接中継装置からシグネチャを受信した中継装置109は、自己に送信した隣接中継装置にはシグネチャを送信しない。

[0124] このようなシグネチャの送信が行われると、図24に示す例では、中継装置109－3は、隣接中継装置となる中継装置109－1および中継装置109－2から同一のシグネチャを受信することになる。また、これと同様に、中継装置109－2も、隣接中継装置となる中継装置109－1および中継装置109－3から同一のシグネチャを受信することになる。その結果、中継装置109－2および中継装置109－3では、重複したシグネチャに基づいたパケット制御処理を行うことになり、シグネチャに基づいたパケットの規制に関する処理を効率的に行うことができない。

[0125] また、図25に示すように、中継装置109－1は、2つの通信端末130がネットワーク

上のサーバ120に対するDDoS攻撃を行っていることを検出すると(同図の(1)参照)、シグネチャを隣接中継装置となる中継装置109－2および中継装置109－3に送信する(同図の(2)参照)。そして、隣接中継装置となる中継装置109－1からシグネチャを受信した中継装置109－2および中継装置109－3は、受信したシグネチャに基づいてパケットを処理するとともに、シグネチャをそれぞれの隣接中継装置となる中継装置109－4に送信する(同図の(3)参照)。

[0126] このようなシグネチャの送信が行われると、図25に示す例では、中継装置109－4は、隣接中継装置となる中継装置109－2および中継装置109－3から同一のシグネチャを受信することになる。その結果、中継装置109－2および中継装置109－3では、重複したシグネチャに基づいたパケット制御処理を行うことになり、シグネチャに基づいたパケットの規制に関する処理を効率的に行うことができない。

[0127] そこで、本実施例2は、上述した従来技術の課題を解決するためになされたものであり、シグネチャの重複登録や重複送信を回避し、シグネチャに基づいたパケット制御を効率的に行うことが可能な中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムを提供することを目的とする。

[0128] [システムの概要および特徴]

次に、図10を用いて、本実施例2に係るネットワーク攻撃防御システムの概要および特徴を説明する。図10は、本実施例2に係るネットワーク攻撃防御システムの構成を示すシステム構成図である。

[0129] 同図に示すように、このネットワーク攻撃防御システム100aは、ネットワーク上に複数の中継装置110を備えて構成される。また、このネットワーク上には、DoS攻撃やDDoS攻撃の対象となるコンピュータとしてのサーバ120や、かかるDoS攻撃やDDoS攻撃を行い得るコンピュータとしての通信端末130が接続されている。なお、以下では、図示した中継装置110の各々を区別する場合には、それぞれ中継装置110－1～中継装置110－7とし、サーバ120の各々を区別する場合には、サーバ120－1またはサーバ120－2とし、通信端末130の各々を区別する場合には、通信端末130－1～通信端末130－5として記載する。

[0130] ここで、中継装置110の原則的な機能を最初に説明すると、中継装置110は、通信

端末130のうち少なくとも1つ以上の通信端末130がネットワーク上のサーバ120に対してDoS攻撃またはDDoS攻撃を行っていることを検出した場合に、パケットの通過を制御するためのシグネチャ(容疑シグネチャや不正シグネチャ)を生成するとともに、パケットの通過を許可するための正規シグネチャを生成する。そして、中継装置110は、自ら生成したシグネチャ(容疑シグネチャ、不正シグネチャおよび正規シグネチャ)をシグネチャリストに登録する。

[0131] また、中継装置110は、生成した容疑シグネチャ(さらには、正規シグネチャの生成に用いた正規条件)を隣接中継装置に送信する。さらに、中継装置110は、容疑シグネチャの生成直後だけでなく、送信ミスや内容更新等に起因して容疑シグネチャを再送信する必要が生じた場合にも、容疑シグネチャ等を改めて隣接中継装置に送信する。

[0132] その一方で、中継装置110は、隣接中継装置から容疑シグネチャ等を受信した場合には、原則として、正規条件に基づいて正規シグネチャを生成するとともに、受信した容疑シグネチャおよび生成した正規シグネチャをシグネチャリストに登録し、さらに、受信した容疑シグネチャおよび正規条件を他の隣接中継装置に送信する。なお、隣接中継装置について例を挙げると、図10において、中継装置110－3における隣接中継装置は、中継装置110－1、中継装置110－2、中継装置110－4および中継装置110－7であり、中継装置110－5および中継装置110－6とは、隣接関係をもたない。また、この隣接関係は、物理的な隣接を意味するものではない。

[0133] このようにして、図10に示したネットワーク攻撃防御システム100aでは、シグネチャを受信した各中継装置110がシグネチャの送信を繰り返すことで、ネットワーク上の全ての中継装置110が同様の容疑シグネチャや正規シグネチャをシグネチャリストに登録することになる。そして、各中継装置110では、かかるシグネチャリストに登録されたシグネチャ基づいてパケットの通過を制御する。つまり、不正シグネチャや容疑シグネチャに該当するパケットについては、伝送帯域を制限して通過させるかもしくは廃棄し、正規シグネチャに該当するパケットやいずれのシグネチャにも該当しないパケットについては、伝送帯域を制限せずに通過を許可する。

[0134] ところで、本実施例2における中継装置110は、上記したような原則的な機能に加

えて、隣接中継装置から受信したシグネチャがシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合に限り、シグネチャをシグネチャリストに登録するとともに隣接中継装置に送信するようにしている点に主たる特徴がある。つまり、隣接中継装置から受信したシグネチャの重複登録や重複送信を回避し、シグネチャに基づいたパケット制御を効率的に行うことができるようにしている。

[0135] ここで、上記の主たる特徴を実現するために中継装置110が備える特徴的な機能を説明すると、容疑のかかる攻撃を検出した中継装置110では、攻撃容疑パケットを制限するための容疑シグネチャおよび容疑シグネチャの生成を一意に識別するための識別情報を生成する。そして、これら容疑シグネチャおよび識別情報を対応付けてシグネチャリストに登録するとともに、生成した容疑シグネチャ(さらには正規条件)および識別情報を隣接中継装置に送信する。さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継先である隣接中継装置を特定するための上流ノードを容疑シグネチャおよび識別情報に対応付けてシグネチャリストに登録する。そして、容疑シグネチャを再送信する必要が生じた場合には、かかるシグネチャリストを参照して、同一の識別情報が付与されたシグネチャを同一の中継先である隣接中継装置に対して再送信する。

[0136] 一方、容疑シグネチャおよび識別情報を受信した中継装置110では、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合には、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置に送信する。さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継元である隣接中継装置を特定するための下流ノードおよび中継先である隣接中継装置を特定するための上流ノードを容疑シグネチャおよび識別情報に対応付けてシグネチャリストに登録する。

[0137] また、容疑シグネチャ等を受信した中継装置110では、上記とは反対に、受信した容疑シグネチャの識別情報がシグネチャリストに既に登録されている場合には、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であるか否かをさらに判定する。そして、下流ノードが同一である場合には、シ

グネチャの再送信であるとして、受信した容疑シグネチャをシグネチャリストに上書き登録するとともに、シグネチャリストに登録されている上流ノードが示す他の隣接中継装置にシグネチャを再送信する。

[0138] その一方、容疑シグネチャ等を受信した中継装置110では、上記した判定において下流ノードが同一でない場合には、シグネチャの再送信でもないとして、受信した容疑シグネチャをシグネチャリストに登録（または上書き登録）することも、他の隣接中継装置に送信（または再送信）することもせず、受信したシグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。そして、かかる既登録通知を隣接中継装置から受信した中継装置110では、シグネチャリストに記憶された上流ノードから当該隣接中継装置に対応する情報（アドレス）を削除する。

[0139] 以下に、図10を用いて、上記した主たる特徴が実現される具体例を説明する。同図に示すように、例えば、通信端末130－4および通信端末130－5がサーバ120－1に対するDoS攻撃を行っており、中継装置110－1が容疑のかかる攻撃を検出したとすると、中継装置110－1は、攻撃容疑パケットを制限するための容疑シグネチャおよび識別情報を生成し、これら容疑シグネチャおよび識別情報を対応付けてシグネチャリストに登録するとともに、生成した容疑シグネチャ（さらには正規条件）および識別情報を隣接中継装置である中継装置110－2および中継装置110－3に送信する。さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継装置110－2および中継装置110－3のアドレスを上流ノードとしてシグネチャリストに登録する（図10の（1）および（2）参照）。

[0140] 一方、中継装置110－2および中継装置110－3は、中継装置110－1から容疑シグネチャおよび識別情報を受信すると、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているか否かを判定するが、ここでは、識別情報が未だ登録されていないので、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置に送信する。つまり、中継装置110－2は、中継装置110－4に容疑シグネチャおよび識別情報を送信し、また、中継装置110－3は、中継装置110－4および中継装置110

－7に容疑シグネチャおよび識別情報を送信する（同図の（3）および（4）参照）。

[0141] さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継装置110－2および中継装置110－3は、下流ノードおよび上流ノードの情報をシグネチャリストに登録する。つまり、中継装置110－2は、中継装置110－1のアドレスを下流ノードとして、中継装置110－4のアドレスを上流ノードとしてシグネチャリストに登録し、また、中継装置110－3は、中継装置110－1のアドレスを下流ノードとして、中継装置110－4および中継装置110－7のアドレスを上流ノードとしてシグネチャリストに登録する。

[0142] そして、中継装置110－7は、中継装置110－3から容疑シグネチャおよび識別情報を受信すると、受信した容疑シグネチャの識別情報は自己のシグネチャリストに未だ登録されていないので、上記した中継装置110－2および中継装置110－3と同様、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するが、隣接中継装置がないので、当該容疑シグネチャおよび識別情報を隣接中継装置に送信することはしない。さらに、中継装置110－7は、上流ノードは登録しないが、中継装置110－3のアドレスを下流ノードとしてシグネチャリストに登録する（同図の（5）参照）。

[0143] その一方、中継装置110－4は、例えば、中継装置110－2から中継装置110－3よりも先に容疑シグネチャおよび識別情報を受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに未だ登録されていないので、上記した中継装置110－2および中継装置110－3と同様、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置となる中継装置110－3、中継装置110－5および中継装置110－6に送信する。さらに、中継装置110－4は、中継装置110－2のアドレスを下流ノードとしてシグネチャリストに登録するとともに、中継装置110－3、中継装置110－5および中継装置110－6のアドレスを上流ノードとしてシグネチャリストに登録する（同図の（6）および（7）参照）。

[0144] そして、中継装置110－5および中継装置110－6は、中継装置110－4から容疑シグネチャおよび識別情報を受信すると、受信した容疑シグネチャの識別情報が自

己のシグネチャリストに未だ登録されていないので、上記した中継装置110－7と同様、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するが、隣接中継装置がないので、当該容疑シグネチャおよび識別情報を隣接中継装置に送信することはしない。さらに、中継装置110－5および中継装置110－6は、上流ノードは登録しないが、中継装置110－4のアドレスを下流ノードとしてシグネチャリストに登録する（同図の（8）参照）。

[0145] ところで、中継装置110－4は、上記した例によって、中継装置110－2から容疑シグネチャおよび識別情報を受信した後、中継装置110－3からも同一の容疑シグネチャおよび識別情報を受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されており、かつ、識別情報に対応付けて登録されている下流ノード（中継装置110－2）が現に受信したシグネチャの下流ノード（中継装置110－3）と同一でないので、受信した容疑シグネチャをシグネチャリストに登録（または上書き登録）することも、他の隣接中継装置に送信（または再送信）することもせず、受信したシグネチャの下流ノードである中継装置110－2に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。そして、かかる既登録通知を中継装置110－4から受信した中継装置110－3では、シグネチャリストに記憶された当該シグネチャの上流ノードから中継装置110－4のアドレスを削除する。

[0146] また、中継装置110－3は、上記した例によって、中継装置110－4からも同一の容疑シグネチャおよび識別情報を受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されており、かつ、識別情報に対応付けて登録されている下流ノード（中継装置110－1）が現に受信したシグネチャの下流ノード（中継装置110－4）と同一でないので、受信した容疑シグネチャをシグネチャリストに登録（または上書き登録）することも、他の隣接中継装置に送信（または再送信）することもせず、受信したシグネチャの下流ノードである中継装置110－4に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。そして、かかる既登録通知を中継装置110－3から受信した中継装置110－4では、シグネチャリストに記憶された当該シグネチャの上流ノード（中継装置110－3、中継装置110

－5および中継装置110－6のアドレス）から中継装置110－3のアドレスを削除する。

[0147] さらに、中継装置110－4は、上記した例によって、中継装置110－2から容疑シグネチャおよび識別情報を受信した後、同じく中継装置110－2から同一の識別情報からなる容疑シグネチャを受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているが、識別情報に対応付けて登録されている下流ノード（中継装置110－2）が現に受信したシグネチャの下流ノード（中継装置110－2）と同一であるので、シグネチャの再送信であるとして、受信した容疑シグネチャをシグネチャリストに上書き登録するとともに、シグネチャリストに登録されている上流ノード（中継装置110－5および中継装置110－6のアドレス）が示す中継装置110－5および中継装置110－6に容疑シグネチャを再送信する。

[0148] 以上のように、図10に示したネットワーク攻撃防御システムでは、隣接中継装置から受信したシグネチャがシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合に限り、シグネチャをシグネチャリストに登録するとともに隣接中継装置に送信するようにすることで、上記した例で言えば、中継装置110－4や中継装置110－3においてシグネチャの重複登録や重複送信が回避され、シグネチャに基づいたパケット制御を効率的に行うことが可能になる。

[0149] なお、中継装置110は、攻撃を防御しながらパケットを中継するための装置であり、例えば、ルータとして機能してもよく、または、ブリッジとして機能してもよい。また、中継装置110は、中継装置110等を管理するための管理用ネットワークに接続されていてもよく、シグネチャは、管理用ネットワークを介して送受されてもよい。さらに、中継装置110が送信するシグネチャは、容疑シグネチャだけに限定されず、中継装置110は、他のシグネチャを送信してもよく、容疑シグネチャに加えて他のシグネチャを送信するようにしてもよい。

[0150] ［中継装置の構成］

次に、図11を用いて、図10に示した中継装置110の構成を説明する。図11は、中継装置110の構成を示すブロック図である。同図に示すように、この中継装置110は、ネットワークインタフェース111と、パケット取得部112と、攻撃検出部113（並びに

攻撃容疑検出条件テーブル113a、不正トラヒック検出条件テーブル113bおよび正規条件テーブル113c)と、シグネチャ通信部114と、識別情報判定部115と、フィルタ部116(並びにシグネチャリスト116a)とを備えて構成される。

[0151] また、中継装置110は、CPU(CentralProcessingUnit)やメモリ、ハードディスク等を有しており、パケット取得部112、攻撃検出部113、シグネチャ通信部114、識別情報判定部115およびフィルタ部116は、CPUによって処理されるプログラムのモジュールであってもよい。また、このプログラムのモジュールは、1つのCPUで処理されてもよく、複数のCPUに分散して処理されてもよい。さらに、中継装置110には、Linux等の汎用OSをインストールしておき、汎用OSに具備されるパケットフィルタをフィルタ部116として機能させてもよい。

[0152] なお、攻撃検出部113は特許請求の範囲に記載の「シグネチャ生成手段」に対応し、シグネチャ通信部114は同じく「シグネチャ通信手段」に対応し、識別情報判定部115は同じく「シグネチャ登録判定手段」に対応し、シグネチャリスト116aは同じく「シグネチャ記憶手段」に対応する。

[0153] 図11において、ネットワークインタフェース部111は、ネットワークと接続されている通信機器との間でパケットを送受する手段であり、具体的には、LAN(LocalAreaNetwork)またはWAN(WideAreaNetwork)などのネットワークと接続するためのネットワーク接続カード等によって構成される。なお、図11には示していないが、キーボードやマウス、マイクなど、ネットワーク管理者から各種の情報や指示の入力を受付ける入力手段や、モニタ(若しくはディスプレイ、タッチパネル)やスピーカなど、各種の情報を出力する出力手段を備えて中継装置110を構成するようにしてもよい。

[0154] パケット取得部112は、ネットワークインタフェース部111が受信したパケットを取得し、取得したパケットの統計に関する統計情報を攻撃検出部113およびパケット数判定部115aに提供する処理部である。

[0155] 攻撃検出部113は、パケット取得部112によって提供された統計情報に基づいて、攻撃の検出および攻撃の分析を行う処理部であり、図11に図示するように、攻撃容疑検出条件テーブル113a、不正トラヒック検出条件テーブル113bおよび正規条件テーブル113cにそれぞれ接続される。ここで、各テーブル113a～113cに記憶され

る情報を具体的に説明した後に、攻撃検出部113による処理内容を説明する。

[0156] 図12は、攻撃容疑検出条件テーブル113aに記憶される情報、より詳細には、受信パケットが攻撃パケットである可能性がある攻撃容疑パケットを検出するために使用される「攻撃容疑検出条件」の一例を示す図である。同図に示すように、攻撃容疑検出条件は、検出属性、検出閾値および検出間隔の組合せからなる複数組(ここでは3組)のレコードで構成され、かかる攻撃容疑検出条件の各レコードの内のいずれかのレコードの条件にトラヒックが一致した場合に、このトラヒックの通信パケットは攻撃容疑パケットであると認識される。なお、番号はレコードを特定するために便宜上使用されるものである。

[0157] 攻撃容疑検出条件の「検出属性」には、例えば、IPパケットに含まれるIPヘッダ部の属性や、IPパケットのペイロード部に含まれるTCPヘッダ部またはUDPヘッダ部の属性が指定される。具体的には、図12において、番号1のレコードの検出属性は、「DestinationIPAddress(宛先IPアドレス)」が「192.168.1.1/32」であり(dst=192.168.1.1/32)、IPの上位層(TCPまたはUDP)のプロトコル種別を示す「Protocol(プロトコル)」が「TCP」であり(Protocol=TCP)、かつ、IPの上位層プロトコルがどのアプリケーションの情報であるかを示す「DestinationPort(宛先ポート番号)」が「80」である(Port=80)という属性値の組で指定される。

[0158] また、番号2のレコード検出属性は、「DestinationIPAddress(宛先IPアドレス)」が「192.168.1.2/32」であり(dst=192.168.1.2/32)、かつ、「Protocol(プロトコル)」が「UDP(UserDatagramprotocol)」である(Protocol=UDP)という属性値の組で指定される。同様に、番号3のレコード検出属性は、「DestinationIPAddress(宛先IPアドレス)」が「192.168.1.0/24」という属性で指定される。

[0159] 攻撃容疑検出条件の「検出閾値」は、同じレコードで指定される検出属性を持つ受信パケットのトラヒックを攻撃容疑トラヒックとして検出するための最低の伝送帯域を指定したものであり、攻撃容疑検出条件の「検出間隔」は、同じく最低の連続時間を指定したものである。なお、図12には示していないが、検出属性においては、「DestinationIPAddress(宛先IPアドレス)」の値を無条件(any)とし、かつ、IPの上位層のプロトコル種別を示す「Protocol(プロトコル)」が「ICMP(InternetControlMessageProtocol)

」となる属性値の組を指定するようにしてもよい。

[0160] 図13は、不正トラヒック検出条件テーブル113bに記憶される情報、より詳細には、攻撃容疑パケットのトラヒックから不正トラヒックを検出するために用いられる「不正トラヒック条件」の一例を示す図である。同図に示すように、不正トラヒック条件は、既知のDDoS攻撃の複数のトラヒックパターンから構成され、攻撃容疑パケットのトラヒックがいずれかのトラヒックパターンに合致した場合に、不正トラヒックであると認識される。なお、番号はレコード(パターン)を特定するために便宜上使用されるものである。

[0161] 具体的には、番号1の不正トラヒック条件は、「伝送帯域T1Kbps以上、パケットがS1秒以上連続送信されている」というトラヒックパターンを示している。また、番号2の不正トラヒック条件は、「伝送帯域T2Kbps以上、ICMP(InternetControlMessageProtocol)上のエコー応答(EchoReply)メッセージのパケットがS2秒以上連続送信されている」というトラヒックパターンを示している。さらに、番号3の不正トラヒック条件は、「伝送帯域T3Kbps以上、データが長すぎるためパケットに含まれるデータは複数IPパケットに分割して送信していることを示すフラグメントパケットがS3秒以上連続送信されている」というトラヒックパターンを示している。

[0162] 図14は、正規条件テーブル113cに記憶される情報、より詳細には、正当な利用者が利用している通信端末130から送信されるパケットを表す「正規条件」の一例を示す図である。同図に示すように、正規条件は、IPパケットにおける属性とそれら属性値の組からなる複数のレコードで構成される。なお、番号はレコード(パターン)を特定するために便宜上使用されるものである。

[0163] 具体的には、番号1のレコードの検出属性は、IPの「SourceIPAddress(送信元IPアドレス)」が「172.16.10.0/24」であることを指定し(src=172.16.10.0/24)、番号2のレコードの検出属性はIP上のサービス品質を示す「TypeofService(サービスタイプ)」が「(16進で)01」であることを指定している(TOS=0x01)。このような正規条件には、例えば、サーバ所有者の会社の支店や、関連会社など、防御対象のサーバ120等の送信元IPアドレスが設定され、サーバ120が収容されているLANの所有者が正規ユーザであると認識しているネットワークの送信元IPアドレスなどが設定される。

[0164] 図11の説明に戻ると、攻撃検出部113は、パケット取得部112によって提供された

統計情報に基づいて攻撃の検出を検出した場合に、攻撃容疑トラヒックの通信パケット(攻撃容疑パケット)を制限するための容疑シグネチャを生成する。具体的には、攻撃検出部113は、図12に示した攻撃容疑検出条件に従って、検出間隔で指定されているより長い時間連続して、検出閾値で指定されている以上の伝送帯域を使用している、検出属性に合致するトラヒックをチェックし、各レコードの内のいずれかのレコードに合致した場合には、このトラヒックを攻撃容疑トラヒックとして検出し、このときに検出された攻撃容疑トラヒックが満たしている攻撃容疑検出条件のレコードの検出属性を容疑シグネチャとして生成する。

[0165] また、攻撃検出部113は、攻撃を検出した場合に、容疑シグネチャとともに正規シグネチャを生成する。具体的には、図14に示した正規条件を参照し、正規条件の全てのレコード毎に、容疑シグネチャとのAND条件をとり、これを正規シグネチャとして生成する。この正規シグネチャは、容疑シグネチャから正規ユーザの通信パケットである正規パケットを許可するために用いられるシグネチャであるが、例えば、図12および図14の例を用いて説明すると、図12における番号1のレコードの条件で検出されるパケットの容疑シグネチャは、[dst=192.168.1.1/32,Protocol=TCP,Port=80]となり、図14において、正規シグネチャは、[src=172.16.10.24,dst=192.168.1.1/32,Protocol=TCP,Port=80]および[TOS=0x01,dst=192.168.1.1/32,Protocol=TCP,Port=80]となる。

[0166] さらに、攻撃検出部113は、図13に示した不正トラヒック条件のいずれかのパターンに合致するトラヒックを検出した場合に、不正トラヒックを制限するための不正シグネチャを生成する。具体的には、検出された不正トラヒック条件を満たすパケットの送信元IPアドレスを不正アドレス範囲として特定し、この不正アドレス範囲であり、かつ、容疑シグネチャに合致するという条件を不正シグネチャとして生成する。

[0167] 上述してきた攻撃検出部113によって生成された容疑シグネチャ、正規シグネチャおよび不正シグネチャは、シグネチャリスト116a(図15参照)に登録される。そして、攻撃検出部113は、各シグネチャの生成を一意に識別するための識別情報を生成し、この識別情報とともにシグネチャをシグネチャリスト116aに登録する。

[0168] ここで、図16を参照して、シグネチャに付与される識別情報を説明する。図16は、

シグネチャに付与される識別情報の例を示す図であるが、同図に示すように、攻撃検出部113は、シグネチャの生成元である中継装置110を一意に識別するための識別子（すなわち、エンジンタイプ、エンジンIDおよびノードIDからなる識別子）および当該中継装置で生成される複数の容疑シグネチャをそれぞれ一意に識別するための識別子（例えば、シーケンシャルに付与される生成番号）から構成される識別情報を生成する。

[0169] 図11において、シグネチャ通信部114は、攻撃検出部113が生成したシグネチャ等を隣接中継装置に送信するとともに、隣接中継装置から送信されたシグネチャを受信し、また、隣接中継装置から受信したシグネチャをシグネチャリスト116aに登録し、さらに、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理部である。

[0170] 具体的には、シグネチャ通信部114は、攻撃検出部113によってシグネチャおよび識別情報がシグネチャリスト116aに登録されると、登録されたシグネチャ等を識別情報とともに隣接中継装置に送信する。さらに、シグネチャ通信部114は、かかるシグネチャおよび識別情報の中継に応じて、中継先である隣接中継装置を特定するための上流ノードをシグネチャおよび識別情報に対応付けてシグネチャリスト116aに登録する（図15参照）。そして、シグネチャ通信部114は、容疑シグネチャ等を再送信する必要が生じた場合には、かかるシグネチャリスト116aを参照して、同一の識別情報が付与されたシグネチャを同一の中継先である隣接中継装置に対して再送信する。

[0171] また、シグネチャ通信部114は、隣接中継装置から受信したシグネチャをシグネチャリスト116aに登録する処理および他の隣接中継装置に送信する処理を行うが、かかる処理は、以下に説明する識別情報判定部115による判定結果に従って実行される。

[0172] 識別情報判定部115は、シグネチャ通信部114によって隣接中継装置からシグネチャを受信した場合に、受信したシグネチャの識別情報がシグネチャリスト116aに既に登録されているか否かを判定する。そして、未だ登録されていないと識別情報判定部115が判定した場合には、上記のシグネチャ通信部114は、受信したシグネチャ

および識別情報をシグネチャリスト116aに登録するとともに、当該シグネチャおよび識別情報を隣接中継装置に送信する。さらに、シグネチャ通信部114は、中継元である隣接中継装置を特定するための下流ノードおよび中継先である隣接中継装置を特定するための上流ノードをシグネチャおよび識別情報に対応付けてシグネチャリスト116aに登録する(図15参照)。

[0173] これとは反対に、受信したシグネチャの識別情報がシグネチャリスト116aに既に登録されている場合には、識別情報判定部115は、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であるか否かをさらに判定する。そして、下流ノードが同一であると識別情報判定部115が判定した場合には、上記のシグネチャ通信部114は、シグネチャの再送信であるとして、受信したシグネチャをシグネチャリスト116aに上書き登録するとともに、シグネチャリスト116aに登録されている上流ノードが示す他の隣接中継装置にシグネチャを再送信する。

[0174] さらに、上記した判定において、下流ノードが同一でないと識別情報判定部115が判定した場合には、上記のシグネチャ通信部114は、シグネチャの再送信でもないとして、受信した容疑シグネチャをシグネチャリスト116aに登録(または上書き登録)することも、他の隣接中継装置に送信(または再送信)することもせず、受信したシグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。その一方、シグネチャ通信部114は、かかる既登録通知を隣接中継装置から受信した場合には、シグネチャリスト116aに記憶された上流ノードから当該隣接中継装置に対応する情報(アドレス)を削除する。

[0175] 図11において、フィルタ部116は、ネットワークインタフェース部111が受信したパケットを受け入れて、シグネチャリスト116aに基づいてパケットの通過(ネットワークインタフェース部111からのパケットの出力)を制御する処理部である。具体的には、入力されたパケットについて、シグネチャリスト116aに登録された「不正シグネチャ」、「正規シグネチャ」、「容疑シグネチャ」のいずれかに該当するか(もしくはいずれにも該当しないか)を判別した上で、該当するシグネチャに基づいてパケットの通過を制御する。

[0176] より詳細には、フィルタ部116は、不正シグネチャに該当するパケットは、不正なパ

ケットを処理するための不正キューに入力し、容疑シグネチャに該当するパケットは、容疑ユーザ用の容疑キューに入力し、正規シグネチャに該当するパケットまたはいずれのシグネチャにも該当しないパケットは、正規ユーザ用の正規キューに入力する。その上で、フィルタ部116は、正規キューに入力されたパケットについては、伝送帯域を制限せずにネットワークインタフェース部111から出力し、容疑キューおよび不正キューに入力されたパケットについては、それぞれのシグネチャ(条件を満たすとして選択されたシグネチャ)が示す伝送帯域制限値に従って制限して出力する。

[0177] なお、フィルタ部116は、シグネチャリスト116aに登録されたシグネチャの検出属性等が所定の解除判断基準を満たした場合には、この所定の解除判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいてパケットの通過を制御する処理を停止する。

[0178] [攻撃容疑パケット検出時の処理]

続いて、図17を参照して、上記した中継装置110による攻撃容疑パケット検出時の動作処理を説明する。図17は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。

[0179] 同図に示すように、中継装置110の攻撃検出部113は、図12に示した攻撃容疑検出条件テーブル113aに基づいて攻撃容疑トラヒックを検出すると(ステップS101)、容疑シグネチャおよび正規シグネチャを生成する(ステップS102)。

[0180] そして、攻撃検出部113は、各シグネチャの生成を一意に識別するための識別情報を生成し(ステップS103)、この識別情報とともに容疑シグネチャおよび正規シグネチャをフィルタ部116のシグネチャリスト116aに登録する(ステップS104)。さらに、シグネチャ通信部114は、攻撃検出部113が生成したシグネチャ等(本実施例2では、容疑シグネチャおよび正規条件)を識別情報とともに隣接中継装置に送信する(ステップS105)。

[0181] なお、シグネチャ通信部114は、上記したステップS104によるシグネチャ等の中継に応じて、中継先である隣接中継装置を特定するための上流ノードをシグネチャリスト116aに登録する。そして、シグネチャ通信部114は、容疑シグネチャ等を再送信する必要が生じた場合には、かかるシグネチャリスト116aを参照して、同一の識別情報

が付与されたシグネチャを同一の中継先である隣接中継装置に対して再送信する。

[0182] [シグネチャ受信時の処理]

続いて、図18を参照して、上記した中継装置110によるシグネチャ受信時の動作処理を説明する。図18は、シグネチャ受信時の処理手順を示すフローチャートである。

[0183] 同図に示すように、中継装置110のシグネチャ通信部114が、隣接中継装置から送信されたシグネチャ等(本実施例2では、容疑シグネチャおよび正規条件)を受信すると(ステップS111)、識別情報判定部115は、受信したシグネチャの識別情報がフィルタ部116のシグネチャリスト116aに既に登録されているか否かを判定し(ステップS112)、さらに、かかる識別情報がシグネチャリスト116aに既に登録されている場合には(ステップS112肯定)、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であるか否かも判定する(ステップS113)。

[0184] かかる判定において、識別情報がシグネチャリスト116aに既に登録されているおり、かつ、下流ノードが同一でないと識別情報判定部115が判定した場合には(ステップS112肯定かつステップS113否定)、シグネチャ通信部114は、受信した容疑シグネチャをシグネチャリスト116aに登録(または上書き登録)することも、他の隣接中継装置に送信(または再送信)することもせず、受信したシグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する(ステップS118)。なお、かかる既登録通知を隣接中継装置から受信した中継装置110では、シグネチャリスト116aに記憶された上流ノードから当該隣接中継装置に対応する情報(アドレス)を削除する。

[0185] これとは反対に、受信したシグネチャの識別情報がシグネチャリスト116aに未だ登録されていないと識別情報判定部115が判定した場合には(ステップS112否定)、シグネチャ通信部114は、受信したシグネチャおよび識別情報をフィルタ部116のシグネチャリスト116aに登録し(ステップS114)、攻撃検出部113は、シグネチャ通信部114が受信した正規条件に基づいて正規シグネチャを生成するとともに(ステップS115)、正規シグネチャをシグネチャリスト116aに登録する(ステップS116)。

[0186] さらに、シグネチャ通信部114は、シグネチャリスト116aに登録した容疑シグネチャおよび識別情報(さらには、正規シグネチャの生成に用いた正規条件)を隣接中継装置に送信する(ステップS117)。なお、シグネチャ通信部114は、このステップS117によるシグネチャ等の中継に応じて、中継元である隣接中継装置を特定するための下流ノードおよび中継先である隣接中継装置を特定するための上流ノードをシグネチャおよび識別情報に対応付けてシグネチャリスト116aに登録する。

[0187] ところで、上記したステップS113の判定において、受信したシグネチャの識別情報がシグネチャリスト116aに既に登録されているが、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であると識別情報判定部115が判定した場合には(ステップS113肯定)、シグネチャ通信部114は、シグネチャの再送信であるとして、受信したシグネチャをシグネチャリスト116aに上書き登録するとともに(ステップS119)、攻撃検出部113は、シグネチャ通信部114が受信した正規条件に基づいて正規シグネチャを再生成するとともに(ステップS120)、正規シグネチャをシグネチャリスト116aに上書き登録する(ステップS121)。さらに、シグネチャ通信部114は、シグネチャリスト116aに登録されている上流ノードが示す他の隣接中継装置に、容疑シグネチャおよび識別情報(さらには、正規シグネチャの生成に用いた正規条件)を再送信する(ステップS122)。

[0188] なお、上記では、シグネチャの再送信であると判定された場合(受信したシグネチャの識別情報がシグネチャリスト116aに既に登録されているが、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一である場合)に、容疑シグネチャの上書き登録、正規シグネチャの再生成および上書き登録(ステップS119～S121)を行う場合を説明したが、本発明は必ずしもこれに限定されるものではなく、これらの処理(ステップS119～S121)を省いて、容疑シグネチャ、識別情報および正規条件の再送信(ステップS122)のみを行うようにしてもよい。

[0189] [不正パケット検出時の処理]

続いて、図19を参照して、上記した中継装置19による不正パケット検出時の動作処理を説明する。図19は、不正パケット検出時の処理手順を示すフローチャートである。

[0190] 同図に示すように、中継装置110の攻撃検出部117が、図13に示した不正トラヒック条件に基づいて不正トラヒックを検出すると(ステップS131)、不正シグネチャを生成する(ステップS132)。そして、攻撃検出部117は、生成した不正シグネチャをフィルタ部116のシグネチャリスト116aに登録する(ステップS133)。

[0191] [パケット制御時の処理]

続いて、図20を参照して、上記した中継装置110によるパケット制御時の動作処理を説明する。図20は、パケット制御時の処理手順を示すフローチャートである。

[0192] 同図に示すように、フィルタ部116は、ネットワークインタフェース部111からパケットが入力されると(ステップS141肯定)、シグネチャリスト116aに登録された不正シグネチャに合致するか否かを判断する(ステップS142)。そして、不正シグネチャに合致した場合には(ステップS142肯定)、フィルタ部116は、不正なパケットを処理するための不正キューにパケットを入力する(ステップS143)。

[0193] これとは反対に、不正シグネチャに合致しない場合には(ステップS142否定)、フィルタ部116は、入力されたパケットが、シグネチャリスト116aに登録された正規シグネチャに合致するか否かを判断する(ステップS144)。そして、正規シグネチャに合致した場合には(ステップS144肯定)、フィルタ部116は、正規なユーザ用の正規キューにパケットを入力する(ステップS145)。

[0194] さらに、この正規シグネチャにも合致しない場合には(ステップS144否定)、フィルタ部116は、入力されたパケットが、シグネチャリスト116aに登録された容疑シグネチャに合致するか否かを判断する(ステップS146)。そして、容疑シグネチャに合致した場合には(ステップS146肯定)、フィルタ部116は、容疑ユーザ用の容疑キューにパケットを入力する(ステップS147)。これとは反対に、容疑シグネチャに合致しない場合には(ステップS146否定)、フィルタ部116は、正規キューにパケットを入力する(ステップS148)。

[0195] そして、フィルタ部116は、それぞれのキューにあるパケットについて、正規キューであれば、伝送帯域を制限せずにネットワークインタフェース部111から出力し、容疑キューおよび不正キューであれば、それぞれのシグネチャが示す伝送帯域制限値に従って制限して出力する。なお、不正シグネチャ、正規シグネチャ、容疑シグネチ

ャの各シグネチャは、それぞれシグネチャリスト116aに複数登録されてもよい。また、登録されたシグネチャの検出属性等が所定の判断基準を満たした場合に、フィルタ部116は、所定の判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいたパケットの通過を制御する処理を停止する。

[0196] [実施例2の効果]

上述してきたように、上記の実施例2によれば、隣接中継装置から受信したシグネチャが既に登録されているか否かを判定して、未だ登録されていないシグネチャのみをシグネチャリスト116aに登録するとともに隣接中継装置に送信するので、シグネチャの重複登録や重複送信が回避され、シグネチャに基づいたパケット制御を効率的に行うことが可能になる。

[0197] また、上記の実施例2によれば、シグネチャの生成を一意に識別するための識別情報を各シグネチャに対応付けて管理するので、シグネチャの具体的な内容にまで踏み込むことなく、識別情報のみからシグネチャが既に登録されているか否かを判定することが可能になる。さらに、シグネチャの内容が同一であっても識別情報(生成元)が異なっていれば、未だ登録されていないシグネチャであるとしてシグネチャリスト116aに登録するとともに隣接中継装置に送信するので、生成元となる各中継装置の性能違い(例えば、攻撃検出や防御解除に係るアルゴリズムの違いなど)が尊重され、安全性の高いパケット制御を行うことが可能になる。

[0198] また、上記の実施例2によれば、攻撃容疑パケットを検出すると、容疑シグネチャおよび識別情報を生成し、これらシグネチャおよび識別情報を隣接中継装置に送信するとともに、中継先である隣接中継装置を特定するための上流オード、識別情報および容疑シグネチャをシグネチャリスト116aに対応付けて登録するので、シグネチャに対して確実に識別情報を付与することが可能になる。さらに、送信ミスや内容更新等に起因してシグネチャを再送信する必要が生じた場合でも、シグネチャリスト116aに登録された上流ノード、識別情報およびシグネチャを参照することで、同一の識別情報が付与されたシグネチャを同一の中継先に対して確実に再送信することが可能になる。

[0199] また、上記の実施例2によれば、隣接中継装置から受信したシグネチャの識別情報

がシグネチャリスト116aに未だ登録されていない場合には、これを他の隣接中継装置に送信するとともに、シグネチャの直前の中継元である隣接中継装置を特定するための下流ノード、シグネチャの直後の中継先である隣接中継装置を特定するための上流ノード、識別情報およびシグネチャをシグネチャリスト116aに対応付けて登録する(図15参照)。そして、隣接中継装置から受信したシグネチャの識別情報がシグネチャリスト116aに既に登録されている場合には、下流ノードが同一であるか否かをさらに判定し、これが同一である場合には、シグネチャをシグネチャリスト116aに上書き登録するとともに、シグネチャリスト116aに登録されている上流ノードが示す他の隣接中継装置にシグネチャを送信するので、送信ミスや内容更新等に起因してシグネチャが再送信されてきた場合でも、このシグネチャを留めることなく、中継先に対して確実に再送信することが可能になる。その一方、下流ノードが同一でない場合には、シグネチャの再送信でもないと判定される結果、シグネチャの重複登録や重複送信を確実に回避することが可能になる。

[0200] また、上記の実施例2によれば、隣接中継装置から受信したシグネチャの識別情報がシグネチャリスト116aに既に登録されており、かつ、下流ノードも同一でない場合には、シグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。さらに、当該既登録通知を他の隣接中継装置から受信した場合には、シグネチャリスト116aに記憶された上流ノードから当該隣接中継装置に対応する情報(アドレス)を削除する。したがって、送信ミスや内容更新等に起因してシグネチャを再送信する必要が生じた場合でも、シグネチャリスト116aから削除された中継先に対してはシグネチャが送信されないことになり、シグネチャの再送信に際してもシグネチャの重複登録や重複送信を確実に回避することが可能になる。

[0201] [他の実施例]

さて、これまで本発明の実施例2について説明したが、本発明は上述した実施例2以外にも、種々の異なる形態にて実施されてよいものである。

[0202] 例えば、上記の実施例2では、シグネチャの生成を一意に識別するための生成識別情報に基づいて重複登録を判定する場合を説明したが、本発明はこれに限定さ

れるものではなく、生成元となる各中継装置の性能を無視し、シグネチャの内容が同一であるか否かによって重複登録を判定するようにしてもよい。さらには、生成元となる各中継装置の性能を考慮し、シグネチャの内容が同一であり、かつ、生成元の性能が同一であるか否かによって重複登録を判定するようにしてもよい。

[0203] また、各中継装置110は、受信した容疑シグネチャおよび識別情報を隣接中継装置に送信する前に、容疑シグネチャの条件を満たすパケットの数が単位時間内に所定の閾値を超過したか否かを判定するようにしてもよい。すなわち、所定の閾値を超過したと判定した場合に初めて(攻撃有りと判定した場合に初めて)、受信した容疑シグネチャを隣接中継装置に送信するようにしてもよい。例えば、図10に示した例で言えば、中継装置110－4は、通信端末130－1～通信端末130－3によって攻撃がなされていないので、中継装置110－2または中継装置110－3から容疑シグネチャおよび識別情報を受信したとしても、所定の閾値を超過したと判定することはなく、容疑シグネチャを隣接中継装置となる中継装置110－5や中継装置110－6に送信しない。

[0204] また、上記の実施例2で図示した各装置(例えば、図10に例示した中継装置110)の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、中継装置110の分散・統合の具体的形態は図示のものに限られず、中継装置110の全部または一部を各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、中継装置110にて行なわれる各処理機能は、その全部または任意の一部が、CPUおよび当該CPUにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

[0205] また、上記の実施例2で説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報(例えば、攻撃容疑検出条件テーブル、不正トラヒック検出条件テーブル、正規条件テーブルの内容等)については、特

記する場合を除いて任意に変更することができる。

[0206] なお、上記の実施例2では、本発明を実現する各装置（例えば、中継装置110）を機能面から説明したが、各装置の各機能はパーソナルコンピュータやワークステーションなどのコンピュータにプログラムを実行させることによって実現することもできる。すなわち、本実施例2で説明した各種の処理手順は、あらかじめ用意されたプログラムをコンピュータ上で実行することによって実現することができる。そして、これらのプログラムは、インターネットなどのネットワークを介して配布することができる。さらに、これらのプログラムは、ハードディスク、フレキシブルディスク（FD）、CD－ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。つまり、例を挙げれば、実施例2に示したような中継装置用プログラムを格納したCD－ROMを配布し、このCD－ROMに格納されたプログラムを各コンピュータが読み出して実行するようにしてもよい。

実施例 3

[0207] 実施例3では、上述した実施例1および実施例2で行うパケット制限処理を組み合わせた場合について説明する。図21は、実施例3に係る中継装置210の構成を示すブロック図である。なお、以下では、実施例1および実施例2に示した中継装置（10および110）と本実施例3に係る中継装置210との相違点について主に説明し、共通点についての説明は省略することとする。

[0208] ［システムの概要および特徴］

図21に示すように、中継装置210は、パケット制限処理を行う処理部として、識別情報判定部215a（実施例2に係る中継装置110の識別情報判定部115に対応）と、パケット数判定部215b（実施例1に係る中継装置10のパケット数判定部15aに対応）と、連続超過回数判定部215c（同じく連続超過回数判定部15bに対応）とを備えている。

[0209] すなわち、中継装置210は、シグネチャの生成を一意に識別するための識別情報を用いて他の中継装置へのパケット中継を制限するとともに、シグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否か、かかる所定の閾値を

連続して超過した回数が所定の閾値を超過したか否かによってパケット中継を制限する。このようにすることで、パケット中継の制限処理を柔軟かつ確実に実行することが可能になる。

[0210] [攻撃容疑パケット検出時の処理]

続いて、図22を参照して、上記した中継装置210による攻撃容疑パケット検出時の動作処理を説明する。図22は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。

[0211] 同図に示すように、中継装置210の攻撃検出部213は、図12に示した攻撃容疑検出条件テーブル113aに基づいて攻撃容疑トラヒックを検出すると(ステップS201)、容疑シグネチャおよび正規シグネチャを生成する(ステップS202)。

[0212] そして、攻撃検出部213は、各シグネチャの生成を一意に識別するための識別情報を生成し(ステップS203)、この識別情報とともに容疑シグネチャおよび正規シグネチャをフィルタ部216のシグネチャリスト216aに登録する(ステップS204)。さらに、シグネチャ通信部214は、攻撃検出部213が生成したシグネチャ等(本実施例3では、容疑シグネチャおよび正規条件)を識別情報とともに隣接中継装置に送信する(ステップS205)。

[0213] なお、シグネチャ通信部214は、上記したステップS204によるシグネチャ等の中継に応じて、中継先である隣接中継装置を特定するための上流ノードをシグネチャリスト216aに登録する。そして、シグネチャ通信部214は、容疑シグネチャ等を再送信する必要が生じた場合には、かかるシグネチャリスト216aを参照して、同一の識別情報が付与されたシグネチャを同一の中継先である隣接中継装置に対して再送信する。

[0214] [シグネチャ受信時の処理]

続いて、図23を参照して、上記した中継装置210によるシグネチャ受信時の動作処理を説明する。図23は、シグネチャ受信時の処理手順を示すフローチャートである。

[0215] 同図に示すように、中継装置210のシグネチャ通信部214が、隣接中継装置から送信されたシグネチャ等(本実施例3では、容疑シグネチャおよび正規条件)を受信すると(ステップS211)、識別情報判定部215aは、受信したシグネチャの識別情報

がフィルタ部216のシグネチャリスト216aに既に登録されているか否かを判定し(ステップS212)、さらに、かかる識別情報がシグネチャリスト216aに既に登録されている場合には(ステップS212肯定)、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であるか否かも判定する(ステップS213)。

[0216] かかる判定において、識別情報がシグネチャリスト216aに既に登録されているおり、かつ、下流ノードが同一でないと識別情報判定部215aが判定した場合には(ステップS212肯定かつステップS213否定)、シグネチャ通信部214は、受信した容疑シグネチャをシグネチャリスト216aに登録(または上書き登録)することも、他の隣接中継装置に送信(または再送信)することもせず、受信したシグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する(ステップS220)。なお、かかる既登録通知を隣接中継装置から受信した中継装置210では、シグネチャリスト216aに記憶された上流ノードから当該隣接中継装置に対応する情報(アドレス)を削除する。

[0217] これとは反対に、受信したシグネチャの識別情報がシグネチャリスト216aに未だ登録されていないと識別情報判定部215aが判定した場合には(ステップS212否定)、シグネチャ通信部214は、受信したシグネチャおよび識別情報をフィルタ部216のシグネチャリスト216aに登録し(ステップS214)、攻撃検出部213は、シグネチャ通信部214が受信した正規条件に基づいて正規シグネチャを生成するとともに(ステップS215)、正規シグネチャをシグネチャリスト216aに登録する(ステップS216)。

[0218] 続いて、パケット数判定部215bは、パケット取得部212によって提供された統計情報から、上記でシグネチャリスト216aに登録した容疑シグネチャの条件を満たすパケットを単位時間毎に取得し、取得したパケットの数が所定の閾値を超過したか否かを判定する(ステップS217)。

[0219] ここで、かかる所定の閾値を超過した場合(ステップS217肯定)、連続超過回数判定部215cは、所定の閾値を連続して超過した回数が、所定値を超過したか否かを判定する(ステップS218)。その結果、かかる所定の閾値を連続して超過した回数が所定値を超過した場合(ステップS218)、シグネチャ通信部214は、シグネチャリスト

216aに登録した容疑シグネチャおよび識別情報（さらには、正規シグネチャの生成に用いた正規条件）を隣接中継装置に送信する（ステップS219）。なお、シグネチャ通信部214は、このステップS219によるシグネチャ等の中継に応じて、中継元である隣接中継装置を特定するための下流ノードおよび中継先である隣接中継装置を特定するための上流ノードをシグネチャおよび識別情報に対応付けてシグネチャリスト216aに登録する。

[0220] また、上記したステップS217において、パケットの数が所定の閾値を超過しなかった場合（ステップS217否定）や、上記したステップS218において、所定の閾値を連続して超過した回数が所定値を超過しなかった場合（ステップS218否定）には、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理（上記のステップS219の処理）は行われない。

[0221] ところで、上記したステップS213の判定において、受信したシグネチャの識別情報がシグネチャリスト216aに既に登録されているが、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であると識別情報判定部215が判定した場合には（ステップS213肯定）、シグネチャ通信部214は、シグネチャの再送信であるとして、受信したシグネチャをシグネチャリスト216aに上書き登録するとともに（ステップS221）、攻撃検出部213は、シグネチャ通信部214が受信した正規条件に基づいて正規シグネチャを再生成するとともに（ステップS222）、正規シグネチャをシグネチャリスト216aに上書き登録する（ステップS223）。

[0222] 続いて、パケット数判定部215bは、パケット取得部212によって提供された統計情報から、上記でシグネチャリスト216aに登録した容疑シグネチャの条件を満たすパケットを単位時間毎に取得し、取得したパケットの数が所定の閾値を超過したか否かを判定する（ステップS224）。

[0223] ここで、かかる所定の閾値を超過した場合（ステップS224肯定）、連続超過回数判定部215cは、所定の閾値を連続して超過した回数が、所定値を超過したか否かを判定する（ステップS225）。その結果、かかる所定の閾値を連続して超過した回数が所定値を超過した場合（ステップS225肯定）、シグネチャ通信部214は、シグネチャリスト216aに登録されている上流ノードが示す他の隣接中継装置に、容疑シグネチ

ャおよび識別情報（さらには、正規シグネチャの生成に用いた正規条件）を再送信する（ステップS226）。

[0224] なお、上記したステップS224において、パケットの数が所定の閾値を超過しなかった場合（ステップS224否定）や、上記したステップS225において、所定の閾値を連続して超過した回数が所定値を超過しなかった場合（ステップS225否定）には、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理（上記のステップS226の処理）は行われない。

[0225] また、上記では、シグネチャの再送信であると判定された場合（受信したシグネチャの識別情報がシグネチャリスト216aに既に登録されているが、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一である場合）に、容疑シグネチャの上書き登録、正規シグネチャの再生成および上書き登録（ステップS221～S223）を行う場合を説明したが、本発明は必ずしもこれに限定されるものではなく、これらの処理（ステップS221～S223）を省いて、上記したステップS224以降の処理のみを行うようにしてもよい。

[0226] さらに、上記では、シグネチャの識別情報を用いた処理の振り分け（例えば、ステップS212）を行った後、所定の閾値を用いた判定処理（例えば、ステップS217やステップS218）を行う場合を説明したが、本発明は必ずしもこれに限定されるものではなく、所定の閾値を用いた判定によって処理を振り分けたうえで、シグネチャの識別情報を用いた判定処理を行うようにしてもよい。

[0227] ［実施例3の効果］

上述したように、上記の実施例3によれば、中継装置は、シグネチャの生成を一意に識別するための識別情報を用いて他の中継装置へのパケット中継を制限するとともに、シグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否か、かかる所定の閾値を連続して超過した回数が所定の閾値を超過したか否かによってパケット中継を制限する。したがって、パケット中継の制限処理を柔軟かつ確実に実行することが可能になる。

産業上の利用可能性

[0228] 以上のように、本発明に係る中継装置、中継方法および中継プログラム並びにネッ

トワーク攻撃防御システムは、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する場合に有用であり、特に、ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことに適する。

請求の範囲

[1] パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置であって、

前記隣接中継装置から受信したシグネチャに基づいて当該シグネチャを他の隣接中継装置に送信すべきか否かを判定し、前記他の隣接中継装置に送信すべきと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信すること

を特徴とする中継装置。

[2] 前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手段と、

前記攻撃有無判定手段によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手段と、

を備えたことを特徴とする請求項1に記載の中継装置。

[3] 前記攻撃有無判定手段は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定手段を備え、

前記シグネチャ送信手段は、前記パケット数判定手段によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項2に記載の中継装置。

[4] 前記攻撃有無判定手段は、前記パケット数判定手段によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定手段をさらに備え、

前記シグネチャ送信手段は、前記連続超過回数判定手段によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項3に記載の中継装置。

[5] 前記シグネチャ送信手段は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする請求項2、3または4に記載の中継装置。

[6] 受信した前記シグネチャを記憶するシグネチャ記憶手段と、

前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、

前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、

を備えたことを特徴とする請求項1に記載の中継装置。

[7] 前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、

前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、

前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする請求項6に記載の中継装置。

[8] 攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手段を備え、

当該シグネチャ生成手段は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする請求項7に記載の中継装置。

[9] 前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を他の隣接中継装置に

送信するとともに、当該シグネチャの直前の中継元である隣接中継装置を特定するための中継元情報、当該シグネチャの直後の中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報および容疑シグネチャを前記シグネチャ記憶手段に対応付けて登録し、

前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されている場合には、当該生成識別情報に対応付けて登録されている中継元情報が前記受信したシグネチャの中継元情報と同一であるか否かをさらに判定し、

前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に既に登録されているが、前記中継元情報が同一であると判定された場合には、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に上書き登録するとともに、当該シグネチャを前記シグネチャ記憶手段に登録されている中継先情報が示す他の隣接中継装置に送信することを特徴とする請求項8に記載の中継装置。

[10] 前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記中継元情報が同一でないと判定された場合には、前記シグネチャの中継元である隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送し、さらに、当該既登録通知を他の隣接中継装置から受信した場合には、前記シグネチャ記憶手段に記憶された中継先情報から当該隣接中継装置に対応する中継先情報を削除することを特徴とする請求項9に記載の中継装置。

[11] パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する複数の中継装置からなるネットワーク攻撃防御システムであって、

前記中継装置は、

前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手段と、

前記攻撃有無判定手段によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手段と

、

を備えたことを特徴とするネットワーク攻撃防御システム。

[12] パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する複数の中継装置からなるネットワーク攻撃防御システムであって、

前記中継装置は、

前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、

前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、

を備えたことを特徴とするネットワーク攻撃防御システム。

[13] パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置における中継方法であって、

前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定工程と、

前記攻撃有無判定工程によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信工程と、

を含んだことを特徴とする中継方法。

[14] 前記攻撃有無判定工程は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定工程を含み、

前記シグネチャ送信工程は、前記パケット数判定工程によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項13に

記載の中継方法。

[15] 前記攻撃有無判定工程は、前記パケット数判定工程によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定工程をさらに含み、

前記シグネチャ送信工程は、前記連続超過回数判定工程によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項14に記載の中継方法。

[16] 前記シグネチャ送信工程は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする請求項13、14または15に記載の中継方法。

[17] パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継方法であって、

前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定工程と、

前記識別情報判定工程によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信工程と、

を含んだことを特徴とする中継方法。

[18] 前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、

前記シグネチャ登録判定工程は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、

前記シグネチャ通信工程は、前記シグネチャ登録判定工程によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に

送信することを特徴とする請求項17に記載の中継方法。

[19] 攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成工程を含み、

当該シグネチャ生成工程は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする請求項18に記載の中継方法。

[20] パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置としてのコンピュータに実行させる中継プログラムであって、

前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手順と、

前記攻撃有無判定手順によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手順と、

をコンピュータに実行させることを特徴とする中継プログラム。

[21] 前記攻撃有無判定手順は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定手順をコンピュータに実行させ、

前記シグネチャ送信手順は、前記パケット数判定手順によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項20に記載の中継プログラム。

[22] 前記攻撃有無判定手順は、前記パケット数判定手順によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定手順をさらにコンピュータに実行させ、

前記シグネチャ送信手順は、前記連続超過回数判定手順によって所定値を超過し

たと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項21に記載の中継プログラム。

[23] 前記シグネチャ送信手順は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする請求項20、21または22に記載の中継プログラム。

[24] パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置としてのコンピュータに実行させる中継プログラムであって、

前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手順と、

前記識別情報判定手順によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手順と、

をコンピュータに実行させることを特徴とする中継プログラム。

[25] 前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、

前記シグネチャ登録判定手順は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、

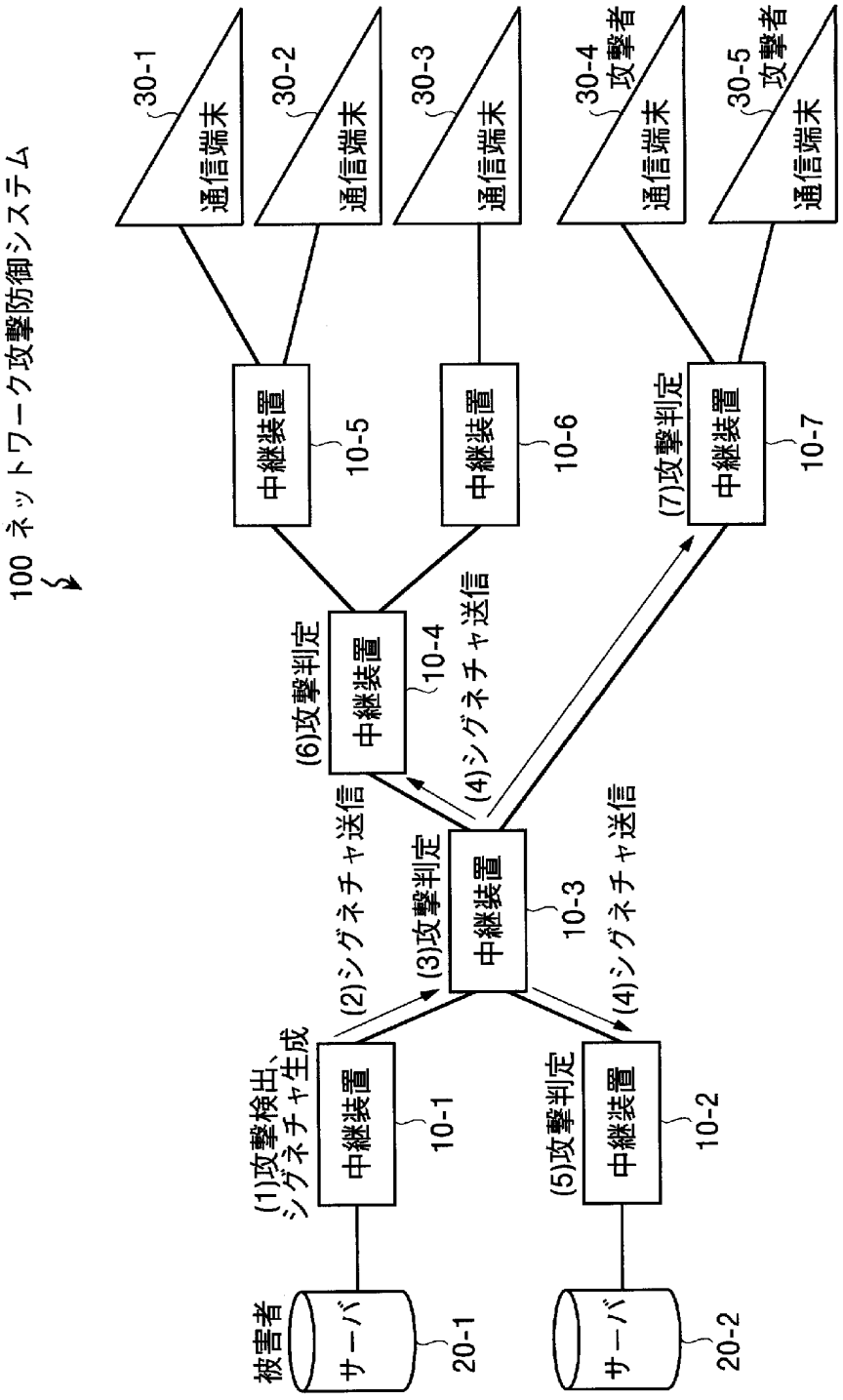
前記シグネチャ通信手順は、前記シグネチャ登録判定手順によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする請求項24に記載の中継プログラム。

[26] 攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手順をコンピュータに実行させ、

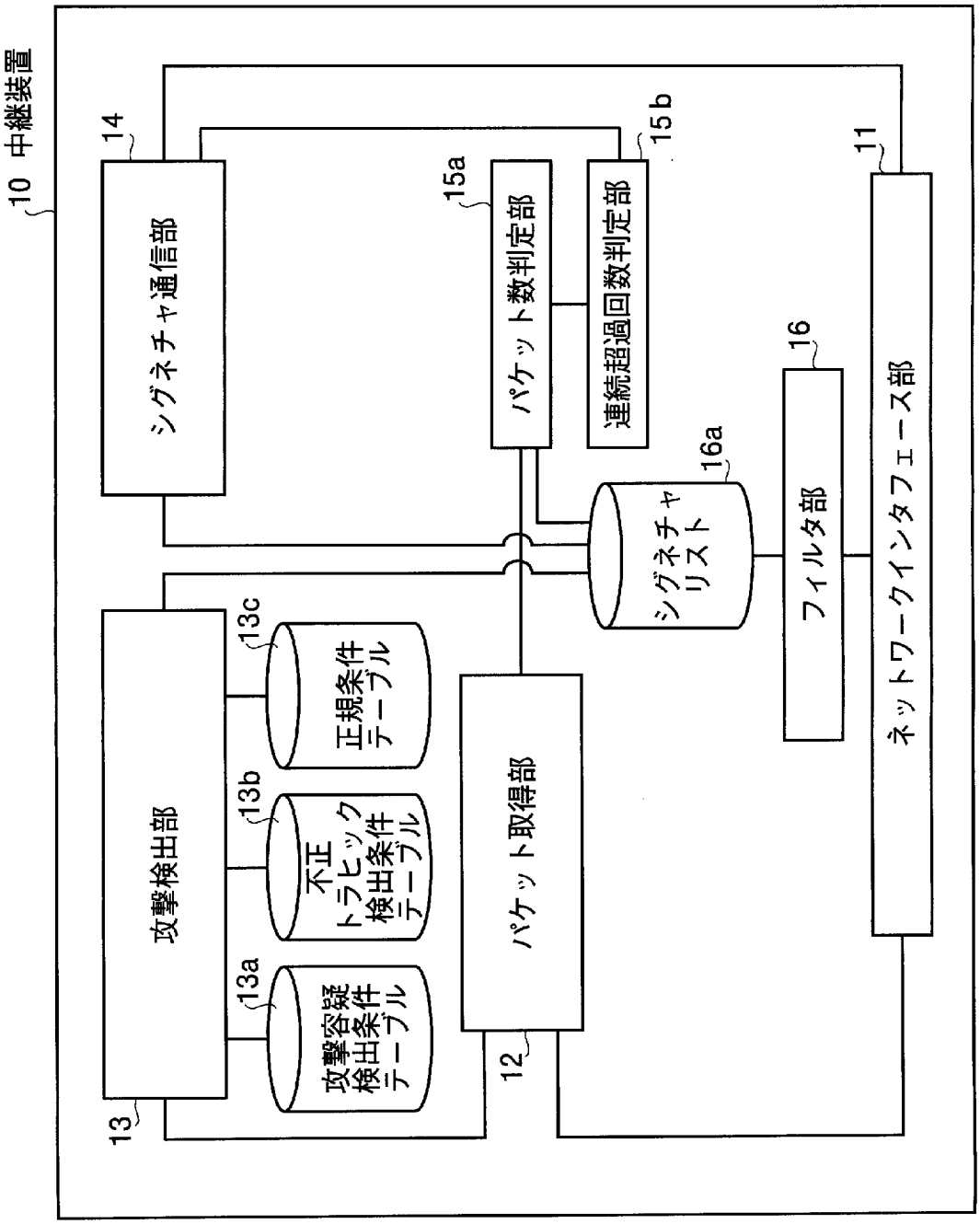
当該シグネチャ生成手順は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報

、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする請求項25に記載の中継プログラム。

[図1]


100 ネットワーク攻撃防御システム
30-1 通信端末
30-2 通信端末
30-3 通信端末
30-4 攻撃者 通信端末
30-5 攻撃者 通信端末
中継装置 10-5
中継装置 10-6
(7)攻撃判定 中継装置 10-7
(6)攻撃判定 中継装置 10-4
(4)シグネチャ送信
(2)シグネチャ送信
(3)攻撃判定 中継装置 10-3
(4)シグネチャ送信
(1)攻撃検出、シグネチャ生成 中継装置 10-1
(5)攻撃判定 中継装置 10-2
被害者 サーバ 20-1
サーバ 20-2

[図2]


10 中継装置
14
シグネチャ通信部
15a
パケット数判定部
15b
連続超過回数判定部
11
ネットワークインタフェース部
16
フィルタ部
16a
シグネチャリスト
攻撃検出部
13
13c
正規条件テーブル
13b
不正トラヒック検出条件テーブル
13a
攻撃容疑検出条件テーブル
パケット取得部
12

[図3]

13a 攻撃容疑検出条件テーブル

番号	検出属性	検出閾値	検出間隔
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500Kbps	10秒
2	{Dst=192.168.1.2/32,Protocol=UDP}	300Kbps	10秒
3	{Dst=192.168.1.1/24}	1000Kbps	20秒
⋮			

[図4]

13b 不正トラヒック条件検出テーブル

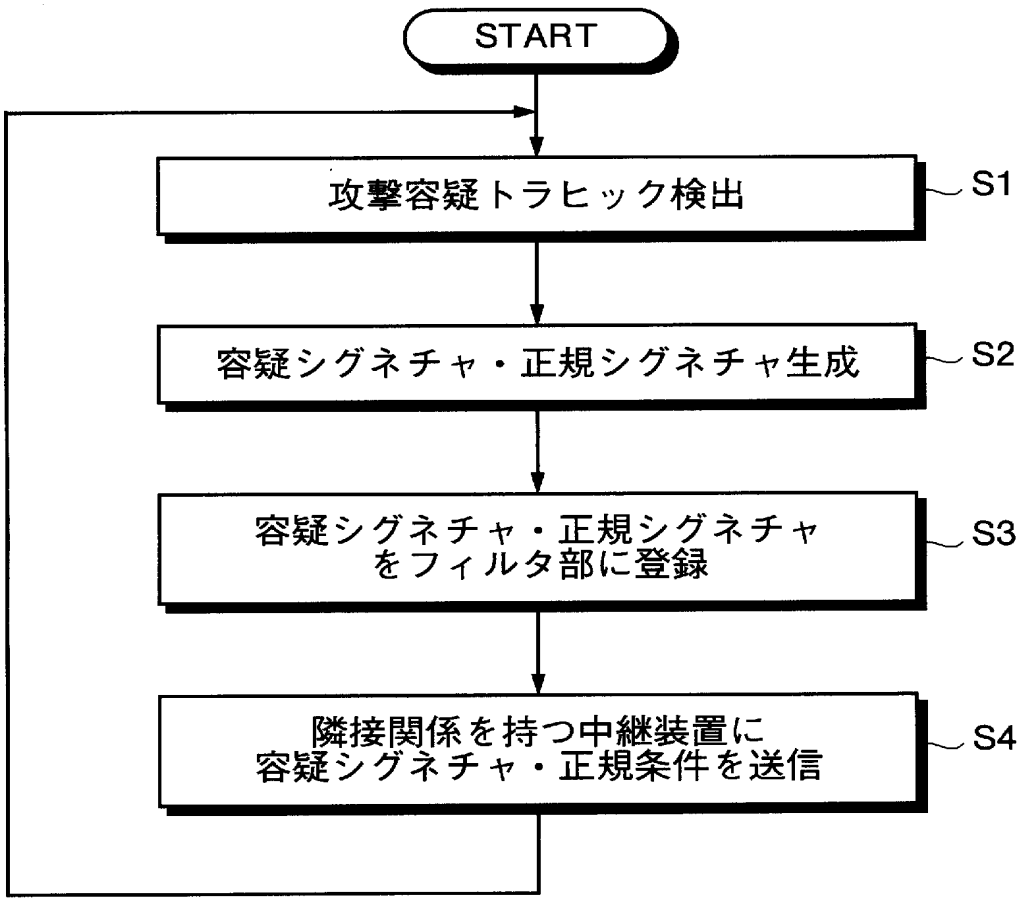
番号	不正トラヒック条件
1	T1Kbps以上のパケットがS1秒以上連続送信されている
2	T2Kbps以上のICMP/Echo Replyパケットが S2秒以上連続送信されている
3	T3Kbps以上のフラグメントパケットが S3秒以上連続送信されている
⋮	

[図5]

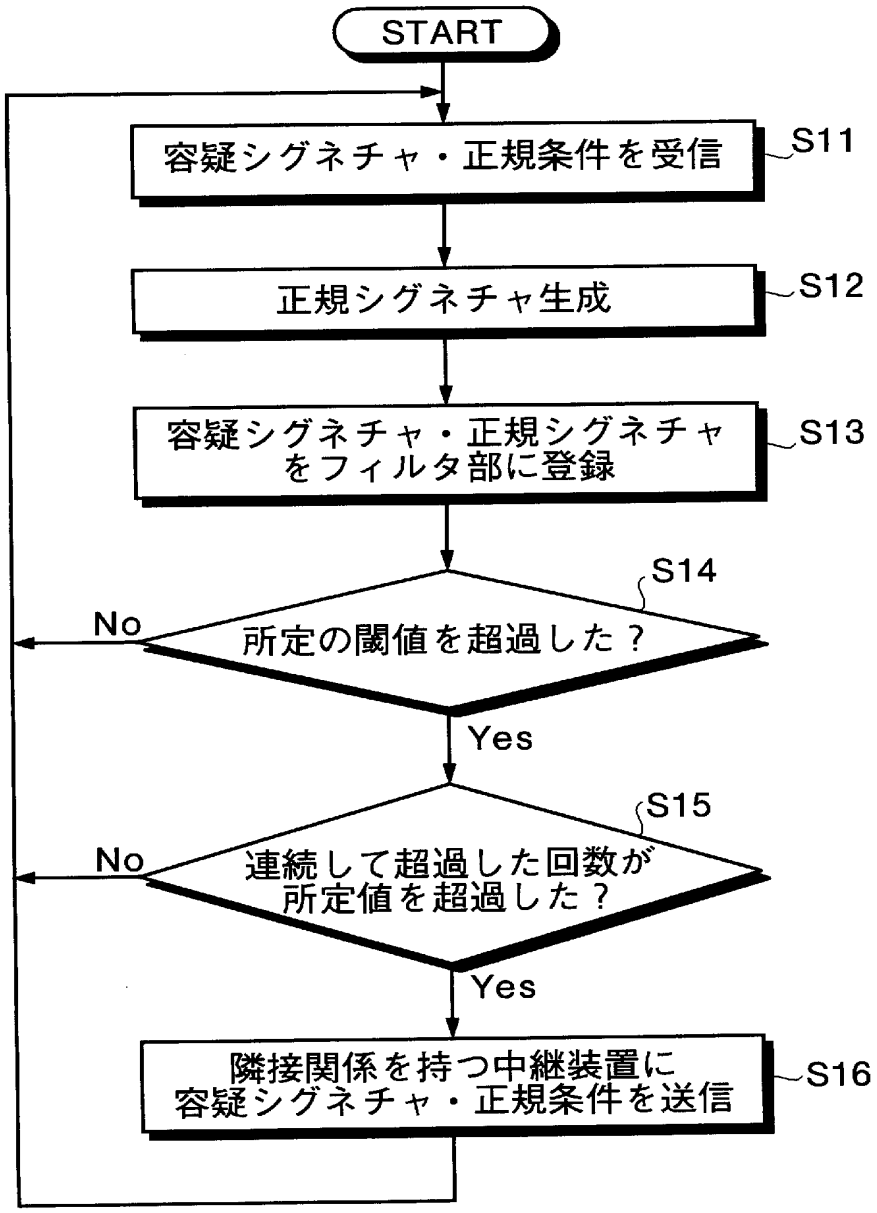
13c 正規条件テーブル

番号	検出属性
1	{Src=172.16.10.0/24}
2	{TOS=0x01}
⋮	

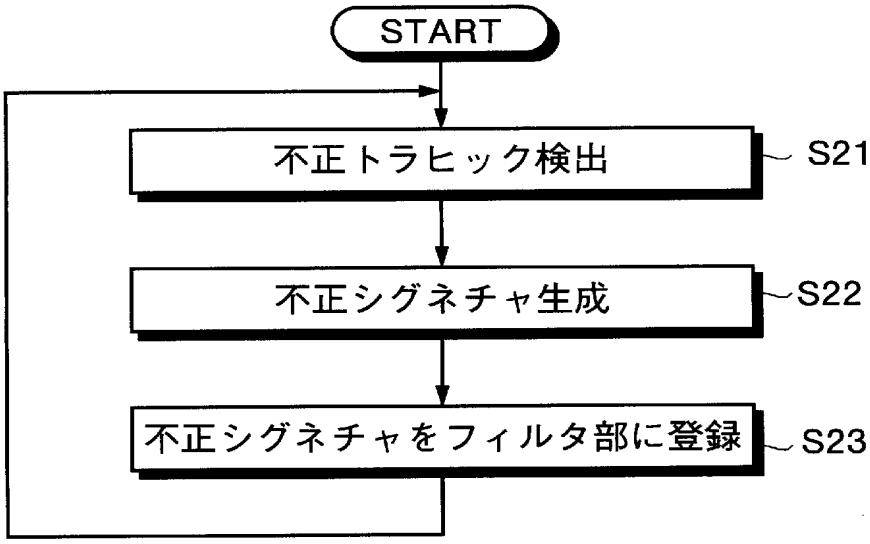
[図6]


START
攻撃容疑トラヒック検出
S1
容疑シグネチャ・正規シグネチャ生成
S2
容疑シグネチャ・正規シグネチャ
をフィルタ部に登録
S3
隣接関係を持つ中継装置に
容疑シグネチャ・正規条件を送信
S4

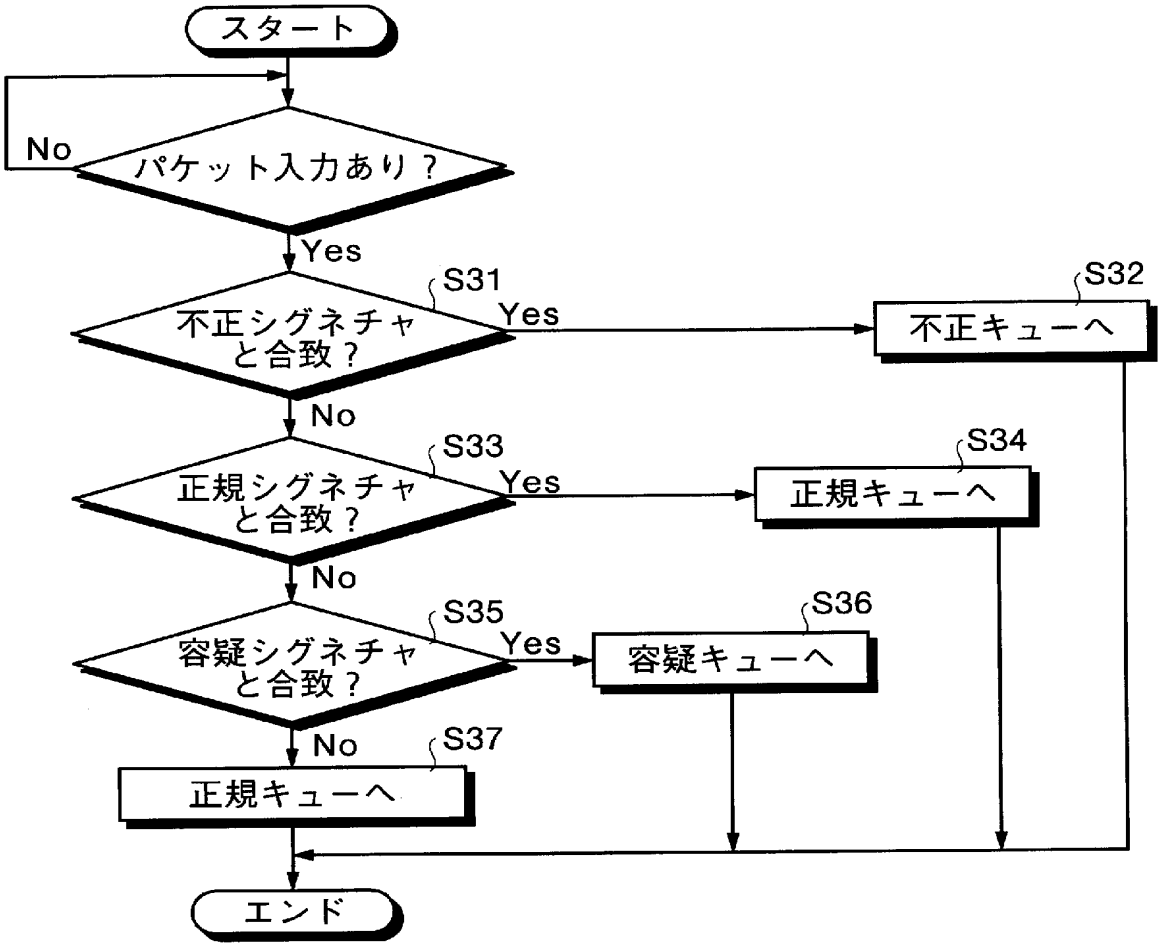
[図7]


START
容疑シグネチャ・正規条件を受信
S11
正規シグネチャ生成
S12
容疑シグネチャ・正規シグネチャ
をフィルタ部に登録
S13
S14
所定の閾値を超過した？
No
Yes
S15
連続して超過した回数が
所定値を超過した？
No
Yes
隣接関係を持つ中継装置に
容疑シグネチャ・正規条件を送信
S16

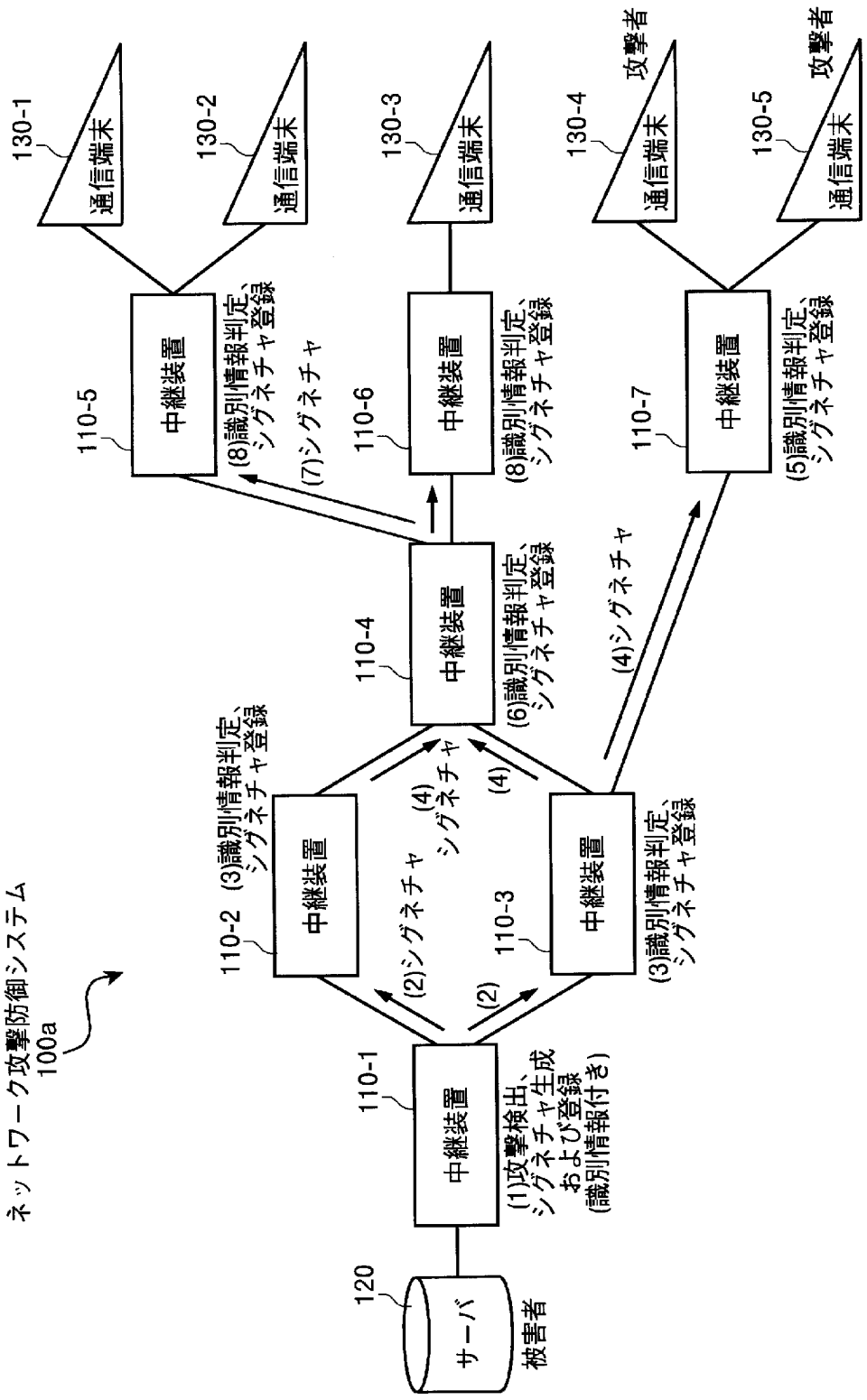
[図8]



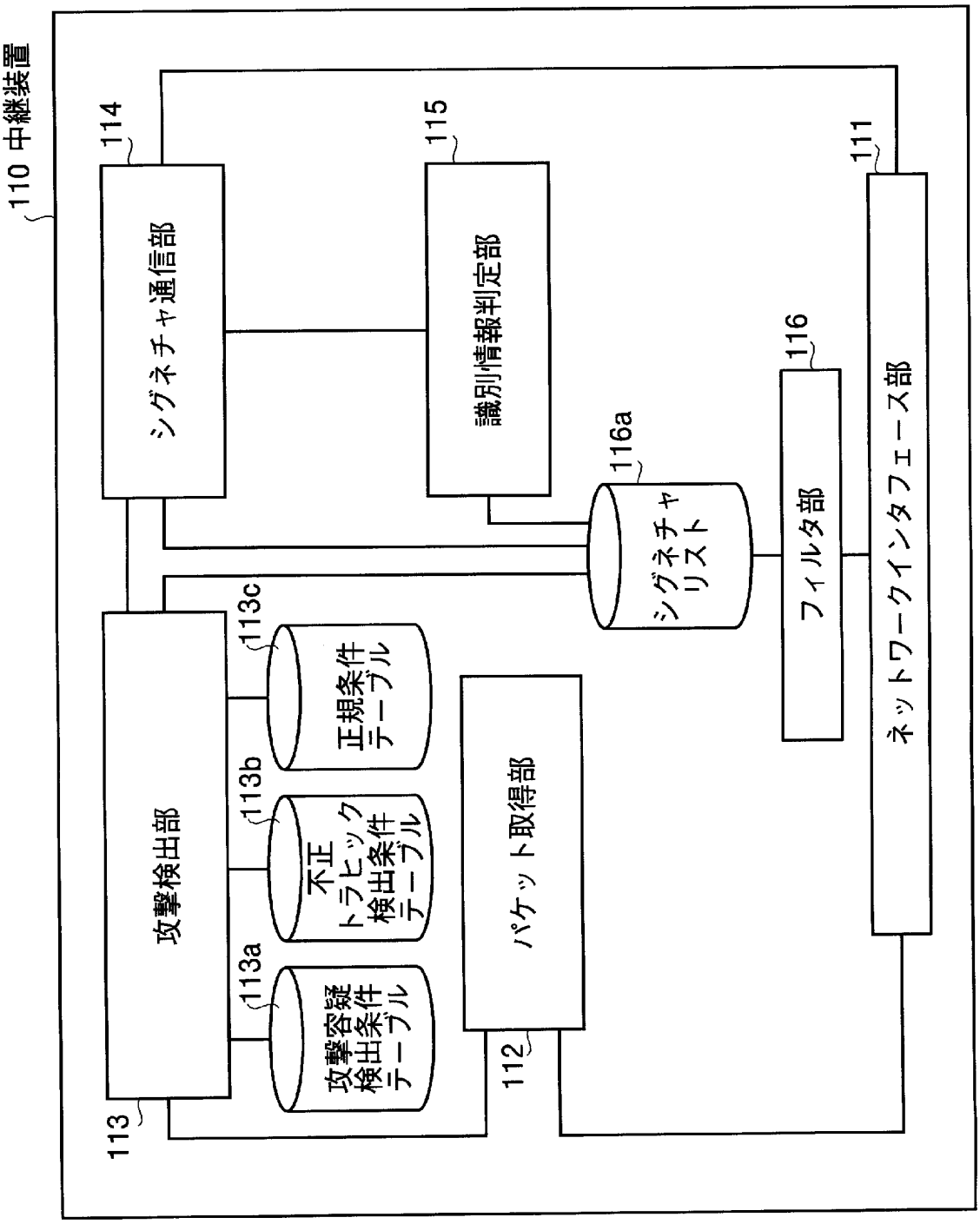
[図9]


スタート
No
パケット入力あり？
Yes
S31
不正シグネチャと合致？
Yes
S32
不正キューへ
No
S33
正規シグネチャと合致？
Yes
S34
正規キューへ
No
S35
容疑シグネチャと合致？
Yes
S36
容疑キューへ
No
S37
正規キューへ
エンド

[図10]


ネットワーク攻撃防御システム
100a
110-1
中継装置
(1)攻撃検出、
シグネチャ生成
および登録
(識別情報付き)
120
サーバ
被害者
(2)シグネチャ
(2)
110-2
中継装置
(3)識別情報判定、
シグネチャ登録
110-3
中継装置
(3)識別情報判定、
シグネチャ登録
(4)
シグネチャ
(4)シグネチャ
110-4
中継装置
(6)識別情報判定、
シグネチャ登録
(6)識別情報判定、
シグネチャ登録
110-5
中継装置
(8)識別情報判定、
シグネチャ登録
(7)シグネチャ
110-6
中継装置
(8)識別情報判定、
シグネチャ登録
110-7
中継装置
(5)識別情報判定、
シグネチャ登録
130-1
通信端末
130-2
通信端末
130-3
通信端末
130-4
攻撃者
通信端末
130-5
攻撃者
通信端末

[図11]


110 中継装置
114
シグネチャ通信部
115
識別情報判定部
111
116
116a
シグネチャリスト
フィルタ部
ネットワークインタフェース部
113c
正規条件テーブル
113b
不正トラヒック検出条件テーブル
113a
攻撃容疑検出条件テーブル
攻撃検出部
113
パケット取得部
112

[図12]

113a 攻撃容疑検出条件テーブル

番号	検出属性	検出閾値	検出間隔
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500Kbps	10秒
2	{Dst=192.168.1.2/32,Protocol=UDP}	300Kbps	10秒
3	{Dst=192.168.1.1/24}	1000Kbps	20秒
⋮			

[図13]

113b 不正トラヒック条件検出テーブル

番号	不正トラヒック条件
1	T1Kbps以上のパケットがS1秒以上連続送信されている
2	T2Kbps以上のICMP/Echo Replyパケットが S2秒以上連続送信されている
3	T3Kbps以上のフラグメントパケットが S3秒以上連続送信されている
⋮	

[図14]

113c 正規条件テーブル

番号	検出属性
1	{Src=172.16.10.0/24}
2	{TOS=0x01}
⋮	

[図15]

116a シグネチャリスト

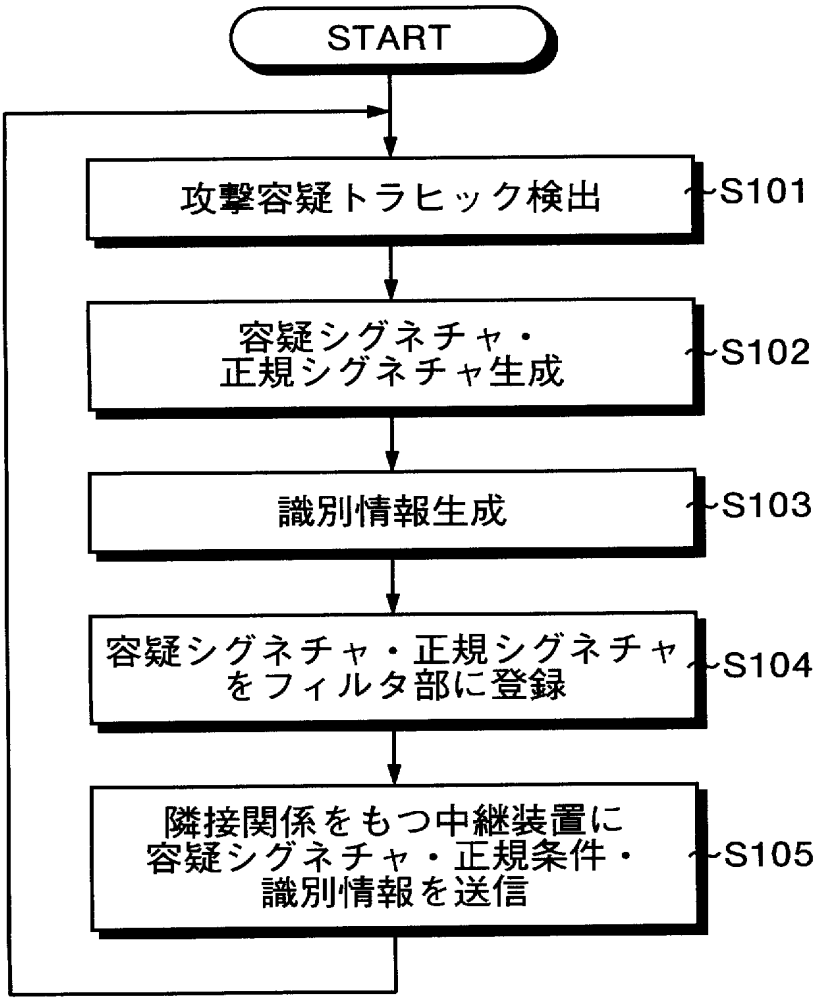
シグネチャ	識別情報	下流ノード	上流ノード
シグネチャA	(…,…,…,…)	中継装置 10-2	中継装置 10-5,10-6
シグネチャB	(…,…,…,…)	中継装置 10-3	中継装置 10-5,10-6
⋮	⋮	⋮	⋮

[図16]

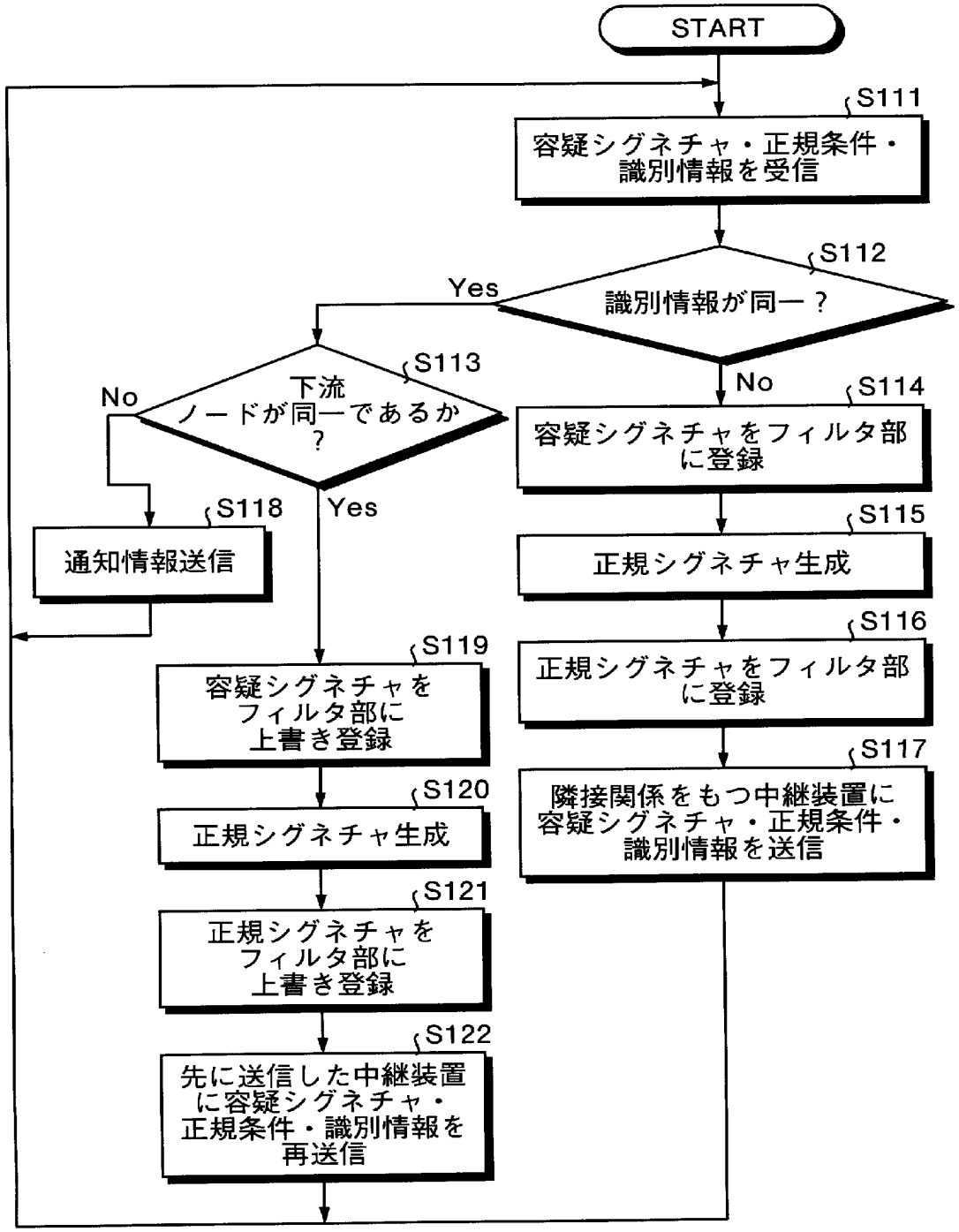
識別情報:{Local Alert ID,Engine-type,Engine-ID,Node-ID}

- Local Alert ID:Analysis Engine内でユニークなAlertの識別子
- Engine-type: Analysis Engineの種類の識別子
- Engine-ID: 同一Mitigationに帰属する同種のAnalysis Engineの識別子
- Node-ID: Analysis Engineが帰属するMitigationのノード識別子

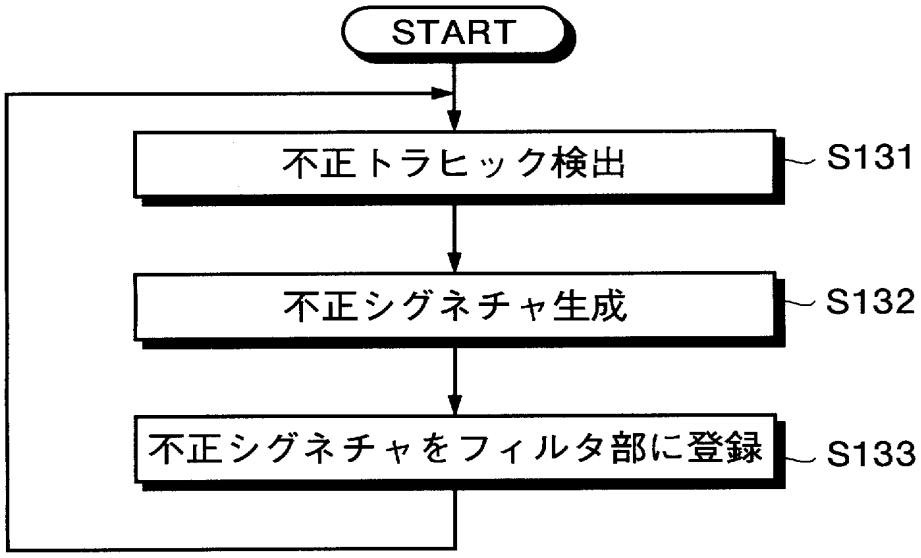
[図17]


START
攻撃容疑トラヒック検出
S101
容疑シグネチャ・
正規シグネチャ生成
S102
識別情報生成
S103
容疑シグネチャ・正規シグネチャ
をフィルタ部に登録
S104
隣接関係をもつ中継装置に
容疑シグネチャ・正規条件・
識別情報を送信
S105

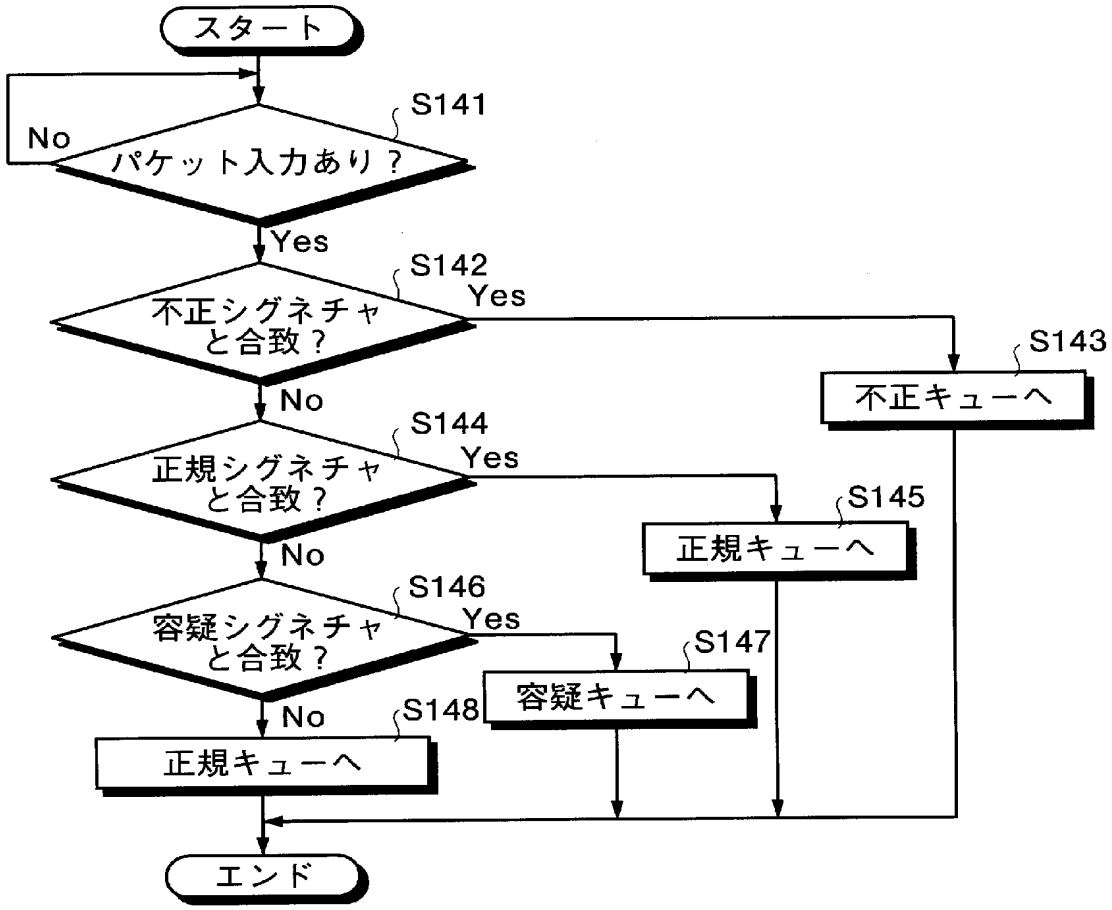
[図18]


START
S111
容疑シグネチャ・正規条件・識別情報を受信
S112
識別情報が同一？
Yes
No
S113
下流ノードが同一であるか？
No
Yes
S114
容疑シグネチャをフィルタ部に登録
S115
正規シグネチャ生成
S116
正規シグネチャをフィルタ部に登録
S117
隣接関係をもつ中継装置に容疑シグネチャ・正規条件・識別情報を送信
S118
通知情報送信
S119
容疑シグネチャをフィルタ部に上書き登録
S120
正規シグネチャ生成
S121
正規シグネチャをフィルタ部に上書き登録
S122
先に送信した中継装置に容疑シグネチャ・正規条件・識別情報を再送信

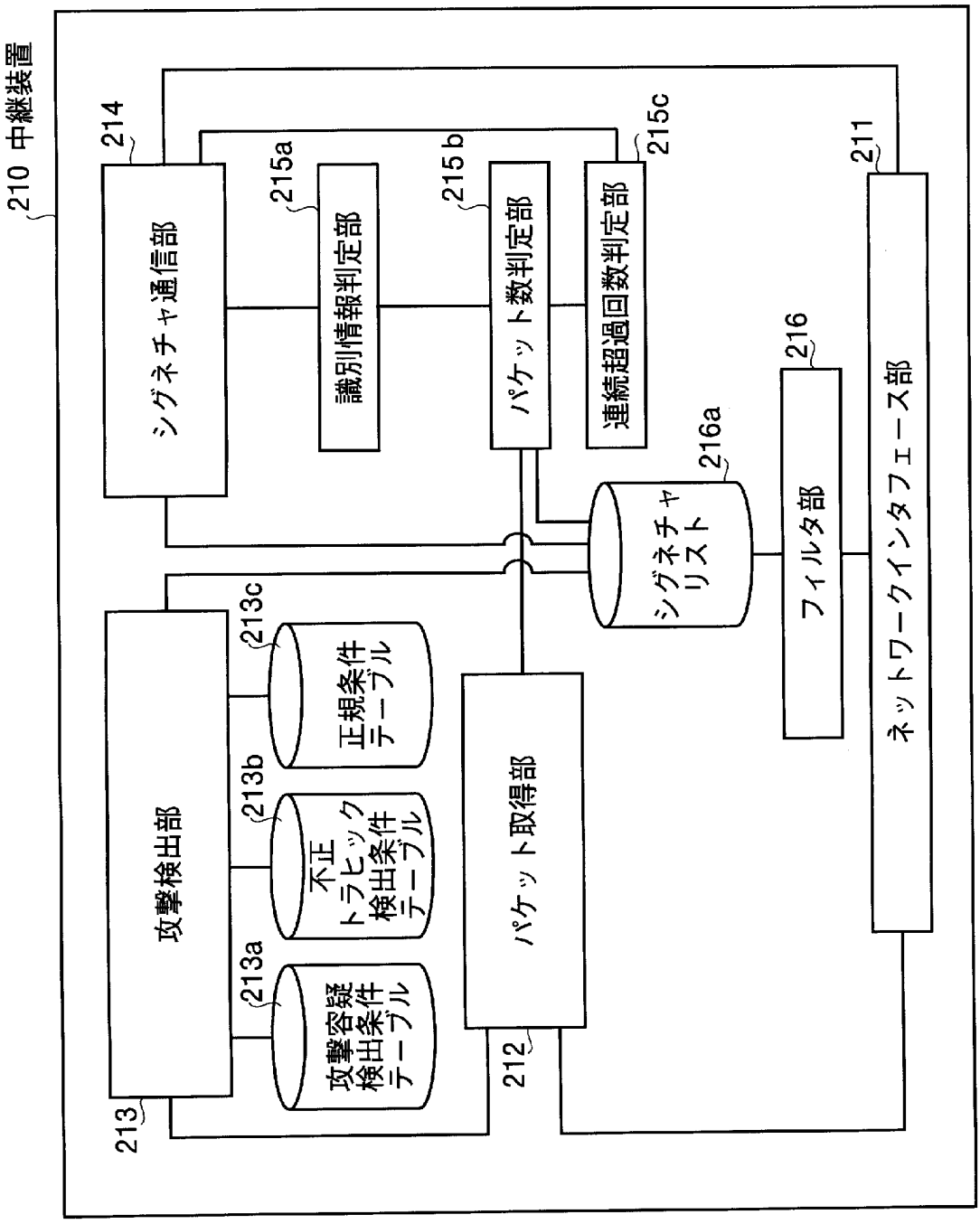
[図19]


START
不正トラヒック検出
S131
不正シグネチャ生成
S132
不正シグネチャをフィルタ部に登録
S133

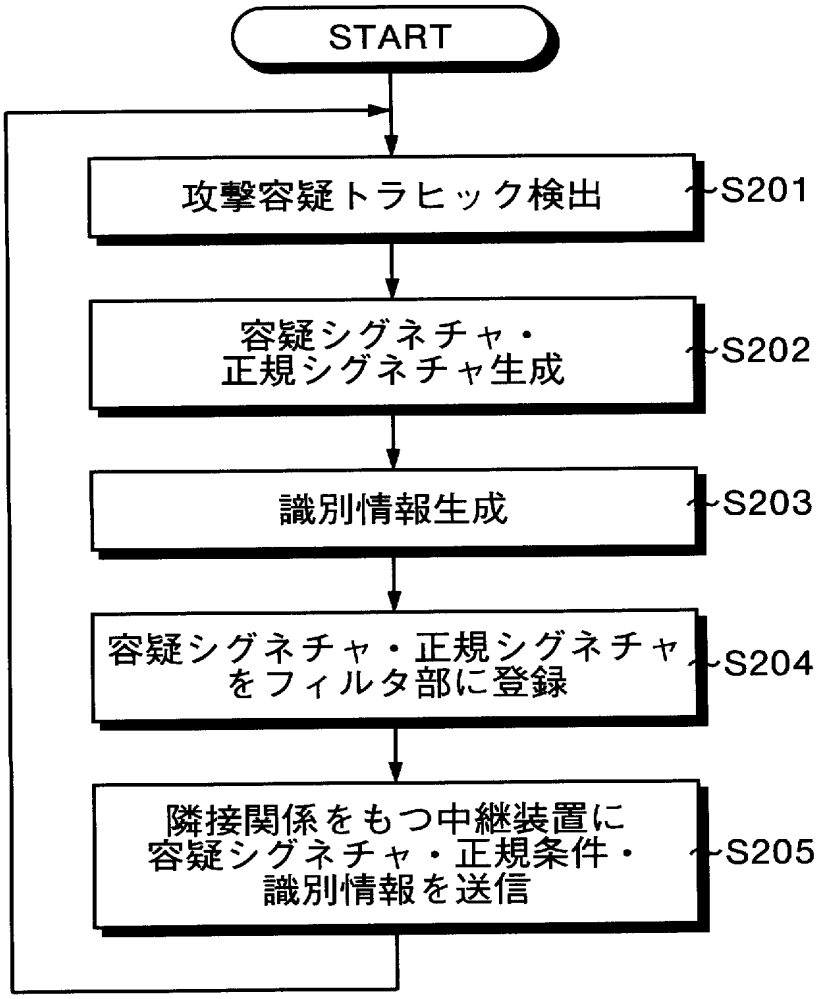
[図20]


スタート
S141
No
パケット入力あり？
Yes
S142
不正シグネチャと合致？
Yes
S143
不正キューへ
No
S144
正規シグネチャと合致？
Yes
S145
正規キューへ
No
S146
容疑シグネチャと合致？
Yes
S147
容疑キューへ
No
S148
正規キューへ
エンド

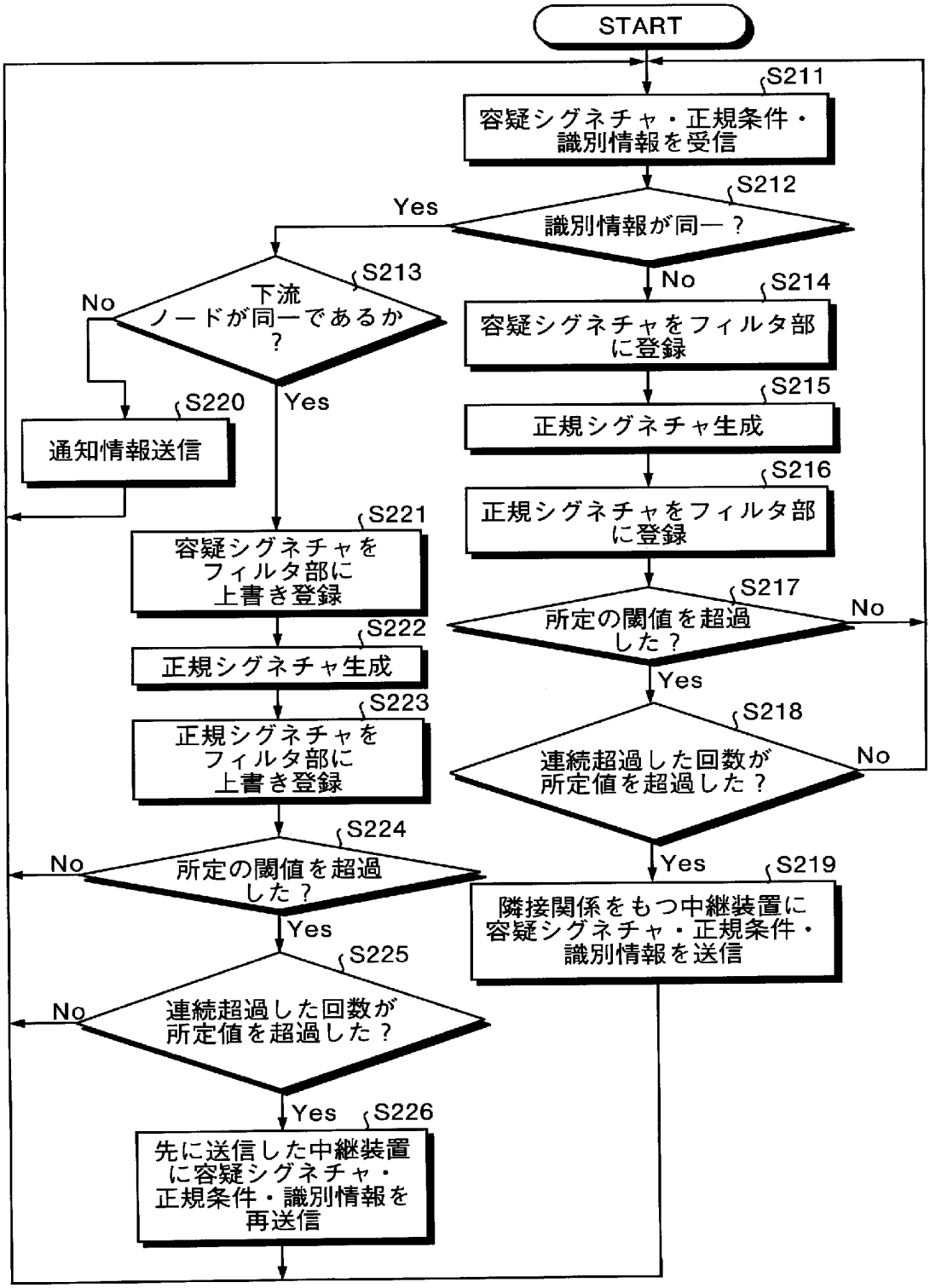
[図21]


210 中継装置
214
シグネチャ通信部
215a
識別情報判定部
215b
パケット数判定部
215c
連続超過回数判定部
211
ネットワークインタフェース部
216
フィルタ部
216a
シグネチャリスト
213
攻撃検出部
213a
攻撃容疑検出条件テーブル
213b
不正トラヒック検出条件テーブル
213c
正規条件テーブル
212
パケット取得部

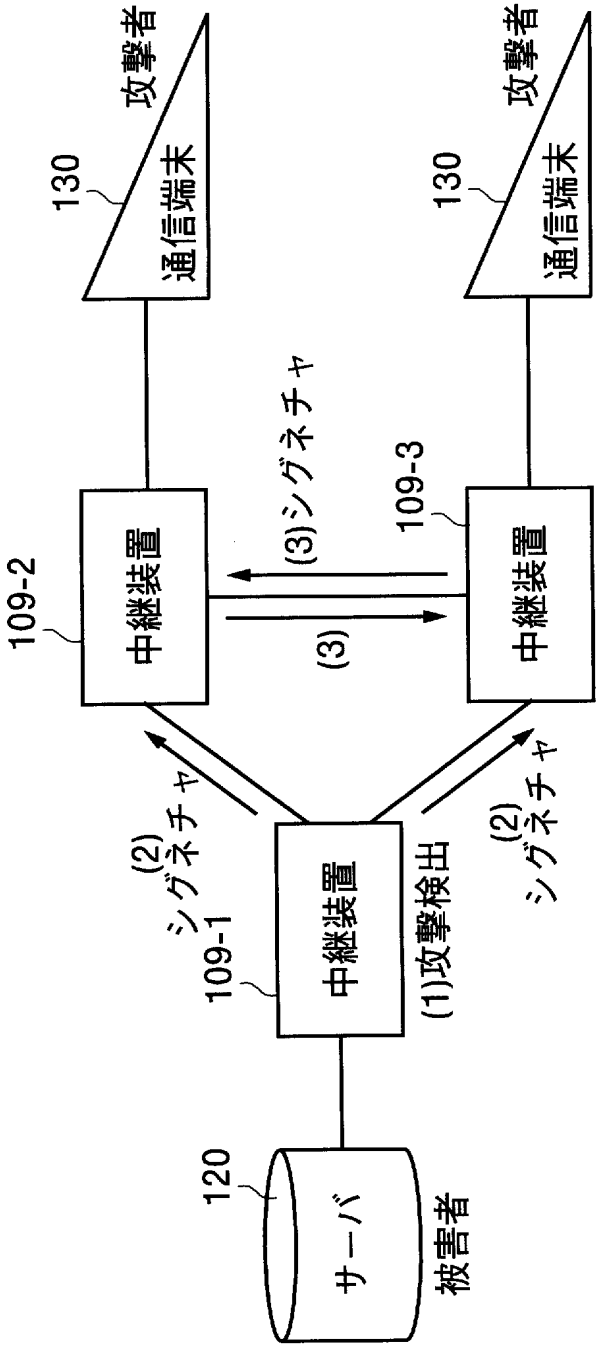
[図22]


START
攻撃容疑トラヒック検出
S201
容疑シグネチャ・
正規シグネチャ生成
S202
識別情報生成
S203
容疑シグネチャ・正規シグネチャ
をフィルタ部に登録
S204
隣接関係をもつ中継装置に
容疑シグネチャ・正規条件・
識別情報を送信
S205

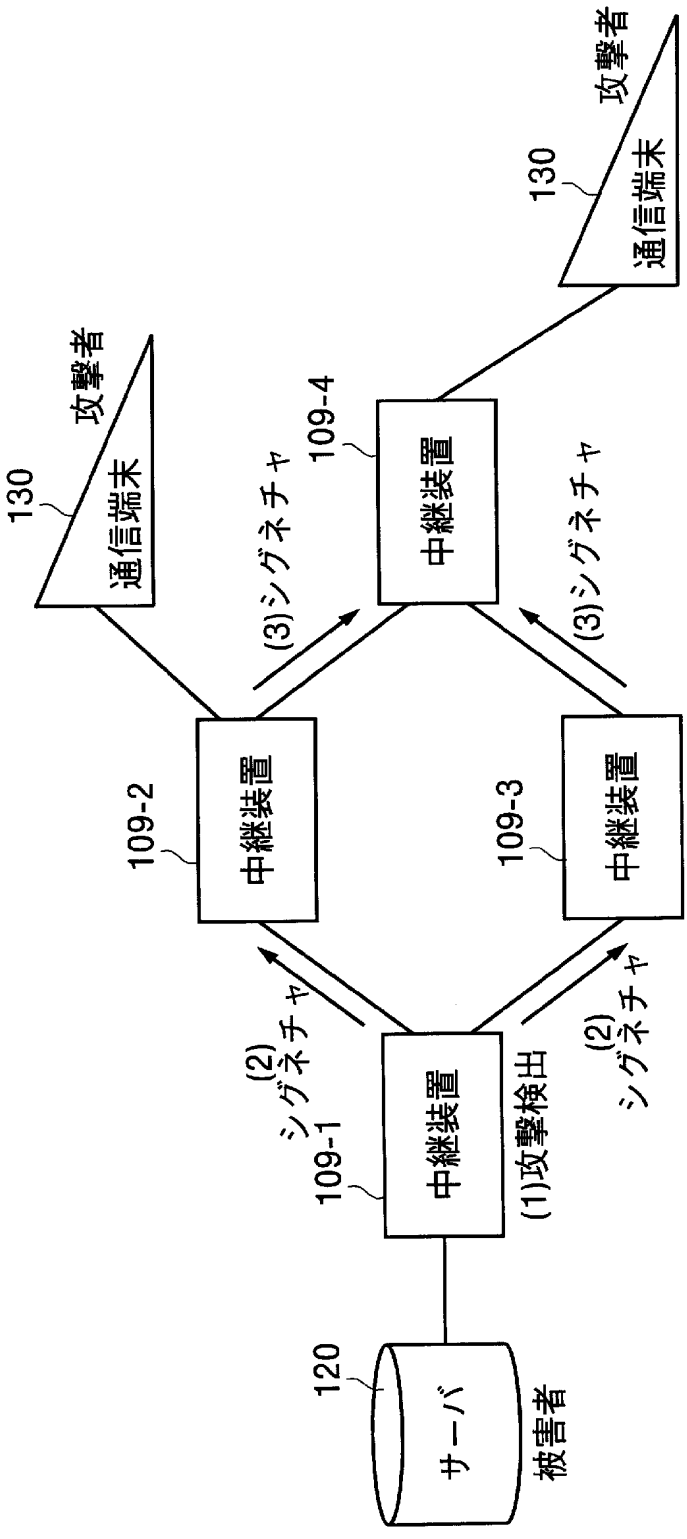
[図23]


START
S211
容疑シグネチャ・正規条件・識別情報を受信
S212
識別情報が同一？
Yes
No
S213
下流ノードが同一であるか？
No
Yes
S214
容疑シグネチャをフィルタ部に登録
S215
正規シグネチャ生成
S216
正規シグネチャをフィルタ部に登録
S217
所定の閾値を超過した？
No
Yes
S218
連続超過した回数が所定値を超過した？
No
Yes
S219
隣接関係をもつ中継装置に容疑シグネチャ・正規条件・識別情報を送信
S220
通知情報送信
S221
容疑シグネチャをフィルタ部に上書き登録
S222
正規シグネチャ生成
S223
正規シグネチャをフィルタ部に上書き登録
S224
所定の閾値を超過した？
No
Yes
S225
連続超過した回数が所定値を超過した？
No
Yes
S226
先に送信した中継装置に容疑シグネチャ・正規条件・識別情報を再送信

[図24]


攻撃者
130
通信端末
攻撃者
130
通信端末
109-2
中継装置
(3)シグネチャ
109-3
(3)
中継装置
(2)
シグネチャ
109-1
中継装置
(1)攻撃検出
(2)
シグネチャ
120
サーバ
被害者

[図25]


攻撃者
通信端末
130
攻撃者
通信端末
130
中継装置
109-4
(3)シグネチャ
(3)シグネチャ
中継装置
109-2
中継装置
109-3
(2)
シグネチャ
(2)
シグネチャ
中継装置
109-1
(1)攻撃検出
サーバ
120
被害者

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/017305

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/66 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L12/66 (2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
IEEE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	KASHIWA, D. Chen, E.Y. Fuji, H., Active shaping: a countermeasure against DDoS attacks, Universal Multiservice Networks, 2002. ECUMN 2002. 2nd European Conference on, 10 April, 2002 (10.04.02), 3.2 BACKTRACK SHAPING, Fig. 4	1-3,5,11,13,14,16,20,21,23 4,6-10,12,15,17-19,22,24-26
X	Chen Eric et al., "Moving Firewall ni Okeru DDoS Kogeki Taisaku System no Hyoka", IEICE technical report, Vol.102, No.350 (IN2002-65), pages 73 to 77, 23 September, 2002 (23.09.02), page 74, (4) Moving FW Software	1,2,5,11,13,16,20,23
A	JP 2003-283554 A (Nippon Telegraph And Telephone Corp.), 03 October, 2003 (03.10.03) (Family: none)	1-26

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 05 October, 2005 (05.10.05)	Date of mailing of the international search report 25 October, 2005 (25.10.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/017305

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-283572 A (Nippon Telegraph And Telephone Corp.), 03 October, 2003 (03.10.03) (Family: none)	1-26

国際調査報告

国際出願番号 PCT／JP2005／017305

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl.[7] *H04L12/66* (2006.01)

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl.[7] *H04L12/66* (2006.01)

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

IEEE

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	Kashiwa, D. Chen, E.Y. Fuji, H., Active shaping: a countermeasure against DDoS attacks, Universal Multiservice Networks, 2002. ECUMN 2002. 2nd European Conference on, 2002.04.10, 3.2 BACKTRACK SHAPING 欄, Fig.4	1-3, 5, 11, 13, 14, 16, 20, 21, 23
A		4, 6-10, 12, 15, 17-19, 22, 24-26

☑ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 05. 10. 2005	国際調査報告の発送日 25.10.2005
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 5X　8525 清水　稔 電話番号　03－3581－1101　内線　3596

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	チェン　エリック 他３名，Ｍｏｖｉｎｇ　ＦｉｒｅｗａｌｌにおけるＤＤｏＳ攻撃対策システムの評価，電子情報通信学会技術研究報告，第102巻，第350号（ＩＮ２００２－６５），p.73-77，2002.09.23，p.74 (4) Moving FW ソフトウェア　欄	1,2,5,11,13,16,20,23
Ａ	ＪＰ ２００３－２８３５５４ Ａ（日本電信電話株式会社） ２００３．１０．０３ （ファミリーなし）	1-26
Ａ	ＪＰ ２００３－２８３５７２ Ａ（日本電信電話株式会社） ２００３．１０．０３ （ファミリーなし）	1-26